(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 340 522 A1

(12) # EUROPEAN PATENT APPLICATION

published in accordance with Art. 153(4) EPC

(43) Date of publication:
20.03.2024 Bulletin 2024/12

(21) Application number: **22815239.3**

(22) Date of filing: **30.05.2022**

(51) International Patent Classification (IPC):
H04W 76/10 *(2018.01)*

(52) Cooperative Patent Classification (CPC):
**H04L 45/00; H04L 45/30; H04L 47/2475;
H04W 76/10**

(86) International application number:
PCT/CN2022/096052

(87) International publication number:
WO 2022/253194 (08.12.2022 Gazette 2022/49)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **04.06.2021 CN 202110625901**

(71) Applicant: **Huawei Technologies Co., Ltd.
Longgang
Shenzhen, Guangdong 518129 (CN)**

(72) Inventors:
- **PENG, Shuping
Shenzhen, Guangdong 518129 (CN)**
- **YANG, Hongjie
Shenzhen, Guangdong 518129 (CN)**
- **ZHOU, Tianran
Shenzhen, Guangdong 518129 (CN)**
- **WU, Peng
Shenzhen, Guangdong 518129 (CN)**
- **LI, Zhenbin
Shenzhen, Guangdong 518129 (CN)**
- **ZHOU, Yu
Shenzhen, Guangdong 518129 (CN)**

(74) Representative: **Pfenning, Meinig & Partner mbB
Patent- und Rechtsanwälte
Theresienhöhe 11a
80339 München (DE)**

(54) # PACKET FORWARDING METHOD AND APPARATUS, AND COMMUNICATION NETWORK

(57) This application provides a packet forwarding method and apparatus, and a communication network, and belongs to the field of communication technologies. In the solutions provided in this application, a controller may obtain a correspondence between an application-aware identifier of a service flow and a network service required for transmitting the service flow, and deliver the correspondence to a network device. Further, when identifying the service flow as a service flow indicated by the application-aware identifier, the network device may directly forward a packet of the service flow by using the corresponding network service. The controller may establish and deliver the correspondence between the application-aware identifier and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

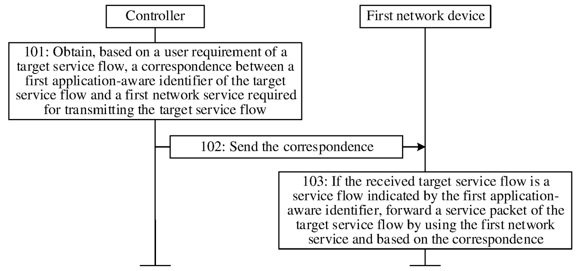

Controller
First network device
101: Obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow
102: Send the correspondence
103: If the received target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence

FIG. 2

EP 4 340 522 A1

Processed by Luminess, 75001 PARIS (FR)

Description

[0001] This application claims priority to Chinese Patent Application No. 202110625901.X, filed on June 4, 2021 and entitled "PACKET FORWARDING METHOD AND APPARATUS, AND COMMUNICATION NETWORK", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] This application relates to the field of communication technologies, and in particular, to a packet forwarding method and apparatus, and a communication network.

BACKGROUND

[0003] In an application-aware network (application-aware networking, APN), a service packet that is of an application and that is sent by a user terminal may carry application-aware information, which is also referred to as application feature information. The application-aware information may include an application-aware identifier and service requirement information. The application-aware identifier may include an application identifier, a user identifier, a flow identifier, and the like. The service requirement information may include a requirement for performance parameters such as a latency, a bandwidth, and a packet loss rate.

[0004] After receiving the service packet that carries the application-aware information, a network device in the APN may forward the service packet based on the application-aware information and in a forwarding manner that can ensure the requirement. However, the forwarding manner of the service packet is single.

SUMMARY

[0005] This application provides a packet forwarding method and apparatus, and a communication network, to resolve a technical problem that a forwarding manner of a service packet is single.

[0006] According to a first aspect, a packet forwarding method is provided, applied to a controller in a network, where the method includes: obtaining, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow; and sending the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow. That is, the first network device may forward the service packet of the target service flow by using the first network service.

[0007] The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence, and provide, for a specific application, a network service that can meet a user requirement corresponding to the application. Therefore, flexibility of forwarding the service packet is effectively improved.

[0008] Optionally, the correspondence includes an identifier of the first network service, and the identifier of the first network service may include: a binding segment identifier (binding segment identifier, BSID) and/or an identifier of a network slice. The BSID may be a BSID of a forwarding path, or may be a BSID of a segment routing (segment routing, SR) policy to which a forwarding path belongs.

[0009] Optionally, the first application-aware identifier may include at least one of a user identifier and an application identifier. The user identifier indicates a user to which the target service flow belongs, and the application identifier indicates an application to which the target service flow belongs.

[0010] Optionally, the first application-aware identifier may further include at least one of a flow identifier, a service level agreement (service level agreement, SLA) level, or a service requirement. The service requirement may be a requirement for performance indicators such as a latency and a packet loss rate, and the flow identifier in the first application-aware identifier is also referred to as a session identifier (session ID).

[0011] Optionally, the method may further include: sending the first application-aware identifier of the target service flow to a second network device, where the first application-aware identifier is used by the second network device to encapsulate the application-aware identifier of the target service flow in the service packet of the target service flow if the second network device determines that the received service flow is the target service flow.

[0012] The second network device may be an application-aware edge device in an APN. After the application-aware edge device encapsulates the application-aware identifier of the target service flow in the service packet of the target service flow, a downstream network device may determine, based on the application-aware identifier, the network service used to forward the target service flow, or may report the application-aware identifier of the target service flow when reporting an in-situ flow detection result of the target service flow.

[0013] Optionally, the method may further include: sending an identifier generation rule to the second network device, so that the second network device generates a second application-aware identifier of the target service flow according to the identifier generation rule, and the second application-aware identifier is used to match the first application-aware identifier to determine that the received service flow is the target service flow.

[0014] The second network device may obtain feature information (for example, 5-tuple information or traffic feature information) that is of the service flow and that is received by the second network device, and process the feature information according to the identifier generation rule delivered by the controller, to generate the second application-aware identifier. Therefore, it can be ensured that the second application-aware identifier accurately matches the first application-aware identifier delivered by the controller. That is, reliability of identifying the target service flow by the second network device is ensured.

[0015] Optionally, the method may further include: obtaining the user requirement of the target service flow through a northbound interface. For example, the controller may obtain, through the northbound interface of the controller, the user requirement that is of the target service flow and that is sent by a frontend.

[0016] Optionally, the method may further include: receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the target application-aware identifier is an application-aware identifier of a service flow to which the in-situ flow detection result belongs, and the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is generated by the network device; and analyzing transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0017] The third network device may be a node on an in-situ flow detection path of the target service flow. The target application-aware identifier may include one or more identifiers, and the controller can analyze the transmission performance of the service flow by using a granularity indicated by at least one of the identifiers, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved.

[0018] Optionally, the method may further include: displaying a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

[0019] The target application-aware identifier may include one or more identifiers, and the controller displays the performance indicator based on the granularity indicated by the at least one identifier. Therefore, refined display of the performance indicator can be implemented, and the display granularity can also be flexibly adjusted.

[0020] Optionally, the method may further include: determining, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; determining that a network service required for transmitting the target service flow is a second network service; and sending a correspondence between the first application-aware identifier and the second network service to the first network device.

[0021] The controller can update, in time based on the detected transmission performance of the target service flow, the network service required for transmitting the target service flow. Therefore, it can be ensured that the updated network service can meet the transmission performance of the target service flow, so that reliable transmission of the target service flow is ensured.

[0022] Optionally, before the receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, the method may further include: sending a sending policy of the target service flow to the first network device and/or the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0023] The controller may deliver the sending policy, so that the network device reports only the in-situ flow detection result of a key service flow. Therefore, a reporting granularity of the in-situ flow detection result is flexibly adjusted, and data processing pressure of the controller is also effectively reduced.

[0024] Optionally, a process of receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device may include: receiving the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device, where the in-situ flow detection flow identifier is also referred to as a monitoring flow identifier, and may indicate a monitored data flow in the target service flow.

[0025] Correspondingly, a process of analyzing transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier may include: determining, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyzing, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0026] The controller may determine, based on the correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, the at least one monitored data flow included in the target service flow, and may further analyze the transmission performance of the target service flow based on the transmission performance of the at least one data flow.

[0027] Optionally, the user requirement of the target service flow includes one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

[0028] According to a second aspect, a packet forwarding method is provided, applied to a network device, where the method includes: receiving a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller in a network, and if a received target service flow is a service flow indicated by the first application-aware identifier, forwarding a service packet of the target service flow by using the first network service and based on the correspondence, where the first application-aware identifier is generated by the controller based on a user requirement of the service flow.

[0029] Optionally, the method further includes: obtaining a second application-aware identifier of the target service flow from the service packet of the target service flow; and if the second application-aware identifier matches the first application-aware identifier, determining that the target service flow is the service flow indicated by the first application-aware identifier.

[0030] Optionally, the service packet received by the network device includes in-situ flow information telemetry (in-situ flow information telemetry, IFIT) information, and the second application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information.

[0031] Alternatively, the second application-aware identifier is encapsulated in a destination address (destination address, DA) field, a hop-by-hop option header (hop-by-hop option header, HBH), a destination option header (destination option header, DOH), or a segment routing header (segment routing header, SRH) of the service packet.

[0032] Optionally, the second application-aware identifier is encapsulated in a binding segment identifier field of the SRH field.

[0033] Optionally, the method further includes: receiving an identifier generation rule sent by the controller; generating a second application-aware identifier of the target service flow according to the identifier generation rule; and if the second application-aware identifier matches the first application-aware identifier, determining that the target service flow is the service flow indicated by the first application-aware identifier.

[0034] Optionally, the service packet received by the network device includes IFIT information; and a process of forwarding a service packet of the target service flow by using the first network service may include: encapsulating a target application-aware identifier in a flow identifier field or a reserved field of the IFIT information; and forwarding, by using the first network service, the service packet in which the target application-aware identifier is encapsulated.

[0035] The network device may further encapsulate the application-aware identifier of the service flow in the IFIT information, so that flexibility of encapsulating the application-aware identifier is improved.

[0036] Optionally, if the service packet that is of the target service flow and that is received by the network device includes in-situ flow detection information, the method may further include: performing in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result; and sending the in-situ flow detection result and the target application-aware identifier to the controller, where the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is obtained by the network device.

[0037] Optionally, the method may further include: receiving a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow. Correspondingly, a process of sending the in-situ flow detection result and the target application-aware identifier to the controller may include: sending the in-situ flow detection result and the target application-aware identifier to the controller based on the indication of the sending policy.

[0038] Optionally, a process of sending the in-situ flow detection result and the target application-aware identifier to the controller may include: sending the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller. The in-situ flow detection flow identifier may indicate a monitored data flow in the target service flow. Therefore, the controller may know a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, so that the controller analyzes transmission performance of at least one data flow included in the target service flow.

[0039] According to a third aspect, a controller is provided, where the controller includes:

a generation module, configured to obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow; and

a sending module, configured to send the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow.

[0040] Optionally, the correspondence includes an identifier of the first network service, and the identifier of the first network service includes: a binding segment identifier and/or an identifier of a network slice.

[0041] Optionally, the first application-aware identifier includes at least one of a user identifier and an application identifier.

[0042] Optionally, the first application-aware identifier further includes at least one of a flow identifier, an SLA level, or a service requirement.

[0043] Optionally, the sending module is further configured to send an identifier generation rule to the first network device, so that the first network device generates a second application-aware identifier of the target service flow according to the identifier generation rule, and the second application-aware identifier is used to match the first application-aware identifier to determine the first network service.

[0044] Optionally, the sending module is further configured to send the first application-aware identifier of the target service flow to a second network device, where the first application-aware identifier is used by the second network device to encapsulate the application-aware identifier of the target service flow in the service packet of the target service flow if the second network device determines that the received service flow is the target service flow.

[0045] Optionally, the controller may further include: an obtaining module, configured to obtain the user requirement of the target service flow through a northbound interface.

[0046] Optionally, the controller may further include:

a receiving module, configured to receive an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the target application-aware identifier is an application-aware identifier of a service flow to which the in-situ flow detection result belongs, and the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is generated by the network device; and

an analysis module, configured to analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0047] Optionally, the controller may further include:

a display module, configured to display a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

[0048] Optionally, the generation module is further configured to: determine, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; and determine that a network service required for transmitting the target service flow is a second network service.

[0049] The sending module is further configured to send a correspondence between the first application-aware identifier and the second network service to the first network device.

[0050] Optionally, before that the receiving module receives an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, the sending module is further configured to send a sending policy of the target service flow to the first network device and/or the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0051] According to a fourth aspect, a network device is provided, where the network device includes:

a receiving module, configured to receive a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller in a network, where the first application-aware identifier is generated by the controller based on a user requirement of a service flow; and

the sending module is configured to: if the received target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence.

[0052] Optionally, the network device may further include:

an obtaining module, configured to obtain a second application-aware identifier of the target service flow from the service packet of the target service flow; and

a determining module, configured to: if the second application-aware identifier matches the first application-aware identifier, determine that the target service flow is the service flow indicated by the first application-aware identifier.

[0053] Optionally, the service packet received by the network device includes IFIT information, and the second application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information.

[0054] Alternatively, the second application-aware identifier is encapsulated in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0055] Optionally, the second application-aware identifier is encapsulated in a binding segment identifier field of the SRH field.

[0056] Optionally, the receiving module may be further configured to receive an identifier generation rule sent by the controller.

[0057] The network device may further include:

a generation module, configured to generate a second application-aware identifier of the target service flow according to the identifier generation rule; and
a determining module, configured to: if the second application-aware identifier matches the first application-aware identifier, determine that the target service flow is the service flow indicated by the first application-aware identifier.

[0058] Optionally, the service packet received by the network device includes IFIT information. The sending module may be configured to: encapsulate the target application-aware identifier in a flow identifier field or a reserved field of the IFIT information, and forward, by using the first network service, the service packet in which the target application-aware identifier is encapsulated.

[0059] Optionally, the network device may further include:
a detection module, configured to: if the service packet that is of the target service flow and that is received by the network device includes in-situ flow detection information, perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result.

[0060] The sending module is further configured to send the in-situ flow detection result and the target application-aware identifier to the controller, where the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is obtained by the network device.

[0061] Optionally, the receiving module may be further configured to receive a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0062] The sending module may be configured to send the in-situ flow detection result and the target application-aware identifier to the controller based on the indication of the sending policy.

[0063] According to a fifth aspect, a packet forwarding method is provided, where the method includes: generating a first application-aware identifier of a target service flow based on a user requirement of the target service flow, and sending the first application-aware identifier. The first application-aware identifier is used by a network device to encapsulate a target application-aware identifier in a service packet of the target service flow, the target application-aware identifier is the first application-aware identifier or a second application-aware identifier matching the first application-aware identifier, the first application-aware identifier corresponds to a first network service, the first application-aware identifier is used by the network device to forward the service packet of the target service flow by using the corresponding first network service, and the first network service meets the user requirement of the target service flow.

[0064] The first application-aware identifier corresponds to the first network service, and is used by the network device to encapsulate the target application-aware identifier in the service packet of the target service flow. Therefore, it can be ensured that the network device that receives the service packet can forward the service packet related to an application by using the first network service corresponding to the specific application, so that flexibility of forwarding the service packet is effectively improved.

[0065] Optionally, a process of generating a first application-aware identifier of a target service flow based on a user requirement of the target service flow may include: A controller in a network generates the first application-aware identifier of the target service flow based on the obtained user requirement of the target service flow. Correspondingly, a process of sending the first application-aware identifier may include: The controller sends the first application-aware identifier to a second network device, so that the second network device encapsulates the target application-aware identifier in the service packet of the target service flow.

[0066] The second network device may be an application-aware edge device in an APN. After the application-aware edge device encapsulates the target application-aware identifier in the service packet of the target service flow, a downstream network device may determine, based on the target application-aware identifier, the first network service used to forward the target service flow.

[0067] Optionally, the method may further include: The controller obtains the user requirement of the target service flow through a northbound interface. For example, the controller may obtain, through the northbound interface of the controller, the user requirement that is of the target service flow and that is sent by a frontend.

[0068] Optionally, the method may further include: The controller determines, based on the user requirement of the target service flow, a first network service required for transmitting the target service flow, and sends a correspondence between the first application-aware identifier and the first network service to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward the service packet of the target service flow.

[0069] The first network device may be a headend network device (also referred to as a head node) of the first network service. For example, the first network device is a head node of a forwarding path, or a head node of a network slice. It should be understood that, the first network device and the second network device may be a same network device, or may be different network devices.

[0070] The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the first network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

[0071] Optionally, the method may further include: The controller receives an in-situ flow detection result and a target application-aware identifier that are sent by a third network device; and analyzes transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0072] The third network device may be a node on an in-situ flow detection path of the target service flow, for example, may be an ingress node, a forwarding node (which may also be referred to as an intermediate node), or an egress node on an in-situ flow detection path. The target application-aware identifier may be the first application-aware identifier, or may be the second application-aware identifier that is of the target service flow and that is generated by the network device.

[0073] When reporting the in-situ flow detection result of the target service flow to the controller, the third network device may also report the target application-aware identifier of the target service flow. Therefore, the controller can further detect and analyze the transmission performance of the service flow by using a granularity indicated by at least one identifier in the target application-aware identifier, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved.

[0074] Optionally, the method may further include: The controller displays a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

[0075] The target application-aware identifier may include one or more identifiers, and the controller displays the performance indicator based on the granularity indicated by the at least one identifier. Therefore, refined display of the performance indicator can be implemented, and the display granularity can also be flexibly adjusted.

[0076] Optionally, a process in which the controller receives an in-situ flow detection result and a target application-aware identifier that are sent by a third network device may include: The controller receives the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device. Correspondingly, a process in which the controller analyzes transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier may include: The controller determines, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and further analyzes, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0077] The controller may determine, based on the correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, the at least one monitored data flow included in the target service flow, and may further analyze the transmission performance of the target service flow based on the transmission performance of the at least one data flow.

[0078] Optionally, the method may further include: The controller determines, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; further determines that a network service required for transmitting the target service flow is a second network service; and further sends a correspondence between the first application-aware identifier and the second network service to the first network device.

[0079] The controller can update, in time based on the detected transmission performance of the target service flow, the network service required for transmitting the target service flow. Therefore, it can be ensured that the updated network service can meet the transmission performance of the target service flow, so that reliable transmission of the target service flow is ensured.

[0080] Optionally, before that the controller receives an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, the method may further include: The controller sends a sending policy of the target service flow to the second network device and/or the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0081] The controller may deliver the sending policy, so that the network device reports only the in-situ flow detection result of a key service flow. Therefore, a reporting granularity of the in-situ flow detection result is flexibly adjusted, and data processing pressure of the controller is also effectively reduced.

[0082] Optionally, a process of generating a first application-aware identifier of a target service flow based on a user requirement of the target service flow may include: A second network device generates the first application-aware identifier of the target service flow based on the user requirement that is of the target service flow and that is sent by a controller. Correspondingly, a process of sending the first application-aware identifier may include: The second network device encapsulates the first application-aware identifier in a service packet of the target service flow, and forwards the service packet in which the first application-aware identifier is encapsulated.

[0083] The second network device may be an application-aware edge device in an APN. After the application-aware edge device generates the first application-aware identifier, and encapsulates the first application-aware identifier in the service packet of the target service flow, a downstream network device may determine, based on the first application-aware identifier, a first network service used to forward the target service flow.

[0084] Optionally, if the service packet that is of the target service flow and that is received by the second network device includes in-situ flow detection information, the method may further include: The second network device performs in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result, and sends the in-situ flow detection result and the first application-aware identifier to the controller.

[0085] Optionally, the method may further include: The second network device receives a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow. A process in which the second network device sends the in-situ flow detection result and the first application-aware identifier to the controller may include: The second network device sends the in-situ flow detection result and the first application-aware identifier to the controller based on the indication of the sending policy.

[0086] Optionally, a process in which the second network device sends the in-situ flow detection result and the first application-aware identifier to the controller may include: The second network device sends the in-situ flow detection result, the first application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

[0087] Optionally, a process in which the second network device encapsulates the first application-aware identifier in a service packet of the target service flow may include: The second network device encapsulates the first application-aware identifier in a flow identifier field or a reserved field of IFIT information of the service packet.

[0088] Alternatively, the second network device encapsulates the first application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet. For example, the second network device may encapsulate the first application-aware identifier in a BSID field of the SRH field.

[0089] Optionally, the user requirement of the target service flow includes one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

[0090] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier. The user identifier indicates a user to which the target service flow belongs, and the application identifier indicates an application to which the target service flow belongs.

[0091] Optionally, the target application-aware identifier may further include at least one of a flow identifier, an SLA level, or a service requirement. The service requirement may be a requirement for performance indicators such as a latency and a packet loss rate, and the flow identifier in the first application-aware identifier is also referred to as a session identifier (session ID).

[0092] According to a sixth aspect, a packet forwarding method is provided, applied to a network device, where the method includes: receiving a first application-aware identifier sent by a controller, where the first application-aware identifier is generated based on a user requirement of a service flow, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the service flow; and if the received target service flow is a service flow indicated by the first application-aware identifier, encapsulating a target application-aware identifier in a service packet of the target service flow, and forwarding the service packet in which the target application-aware identifier is encapsulated. The target application-aware identifier is the first application-aware identifier, or a second application-aware identifier matching the first application-aware identifier.

[0093] Optionally, if the service packet that is of the target service flow and that is received by the network device includes in-situ flow detection information, the method may further include: performing in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result, and sending the in-situ flow detection result and the target application-aware identifier to the controller.

[0094] Optionally, a process of sending the in-situ flow detection result and the target application-aware identifier to the controller may include: sending the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

[0095] Optionally, a process of encapsulating a target application-aware identifier in a service packet of the target service flow may include: encapsulating the target application-aware identifier in a flow identifier field or a reserved field of IFIT information of the service packet; or encapsulating the target application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0096] Optionally, a process of receiving a first application-aware identifier sent by a controller may include: receiving a correspondence that is between the first application-aware identifier and the first network service and that is sent by the controller. Correspondingly, a process of forwarding the service packet in which the target application-aware identifier is encapsulated may include: forwarding, by using the first network service, the service packet in which the target application-aware identifier is encapsulated.

[0097] According to a seventh aspect, a packet forwarding apparatus is provided, where the apparatus includes:

a generation module, configured to generate a first application-aware identifier of a target service flow based on a user requirement of the target service flow, where the first application-aware identifier is used by a network device to encapsulate a target application-aware identifier in a service packet of the target service flow, the target application-aware identifier is the first application-aware identifier or a second application-aware identifier matching the first application-aware identifier, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the target service flow; and
a sending module, configured to send the first application-aware identifier, where the first application-aware identifier is used by the network device to forward the service packet of the target service flow by using the first network service.

[0098] Optionally, the packet forwarding apparatus may be used in a controller in a network, and the generation module is configured to generate the first application-aware identifier of the target service flow based on the obtained user requirement of the target service flow.

[0099] The sending module is configured to send the first application-aware identifier to a second network device, so that the second network device encapsulates the target application-aware identifier in the service packet of the target service flow.

[0100] Optionally, the apparatus further includes: an obtaining module, configured to obtain the user requirement of the target service flow through a northbound interface.

[0101] Optionally, the generation module is further configured to determine, based on the user requirement of the target service flow, the first network service required for transmitting the target service flow.

[0102] The sending module is further configured to send a correspondence between the first application-aware identifier and the first network service to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward the service packet of the target service flow.

[0103] Optionally, the apparatus may further include:

a receiving module, configured to receive an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the target application-aware identifier is an application-aware identifier of a service flow to which the in-situ flow detection result belongs, and the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is generated by the network device; and
an analysis module, configured to analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0104] Optionally, the apparatus may further include:
a display module, configured to display a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

[0105] Optionally, the receiving module may be configured to receive the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by a third network device.

[0106] The analysis module may be configured to: determine, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyze, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0107] Optionally, the generation module may be further configured to: determine, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; and further determine that a network service required for transmitting the target service flow is a second network service.

[0108] The sending module may be further configured to send a correspondence between the first application-aware identifier and the second network service to the first network device.

[0109] Optionally, before that the receiving module receives an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, the sending module may be further configured to send a sending policy of the target service flow to the second network device and/or the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0110] Optionally, the packet forwarding apparatus may be used in the second network device, and the generation module may be configured to generate the first application-aware identifier of the target service flow based on the user requirement that is of the target service flow and that is sent by a controller.

[0111] The sending module may be configured to: encapsulate the first application-aware identifier in a service packet of the target service flow, and forward the service packet in which the first application-aware identifier is encapsulated.

[0112] Optionally, if the service packet that is of the target service flow and that is received by the second network device includes in-situ flow detection information, the apparatus may further include:
a detection module, configured to perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result.

[0113] The sending module may be further configured to send the in-situ flow detection result and the first application-aware identifier to the controller.

[0114] Optionally, the apparatus may further include:
a receiving module, configured to receive a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0115] The sending module may be configured to send the in-situ flow detection result and the first application-aware identifier to the controller based on the indication of the sending policy.

[0116] Optionally, the sending module may be configured to send the in-situ flow detection result, the first application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

[0117] Optionally, the sending module may be configured to: encapsulate the first application-aware identifier in a flow identifier field or a reserved field of IFIT information of the service packet; or encapsulate the first application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0118] Optionally, the user requirement of the target service flow includes one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

[0119] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier.

[0120] According to an eighth aspect, a network device is provided, where the network device includes:

a receiving module, configured to receive a first application-aware identifier sent by a controller, where the first application-aware identifier is generated based on a user requirement of a service flow, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the service flow;
an encapsulation module, configured to: if the received target service flow is a service flow indicated by the first application-aware identifier, encapsulate a target application-aware identifier in a service packet of the target service flow, where the target application-aware identifier is the first application-aware identifier or a second application-aware identifier matching the first application-aware identifier; and
a sending module, configured to forward the service packet in which the target application-aware identifier is encapsulated.

[0121] Optionally, if the service packet that is of the target service flow and that is received by the network device includes in-situ flow detection information, the network device may further include:
a detection module, configured to perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result.

[0122] The sending module is further configured to send the in-situ flow detection result and the target application-aware identifier to the controller.

[0123] Optionally, the sending module may be configured to send the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

[0124] Optionally, the encapsulation module may be configured to: encapsulate the target application-aware identifier in a flow identifier field or a reserved field of IFIT information of the service packet; or encapsulate the target application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0125] Optionally, the receiving module may be configured to receive a correspondence that is between the first application-aware identifier and the first network service and that is sent by the controller. Correspondingly, the sending module may be configured to forward, by using the first network service, the service packet in which the target application-aware identifier is encapsulated.

[0126] According to a ninth aspect, a method for detecting performance of a service flow is provided, applied to a network device, where the method includes: performing, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result; and sending the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller in a network. The target application-aware identifier is generated based on a user requirement of the target service flow, and the in-situ flow detection result and the target application-aware identifier are used by the controller to analyze transmission performance of the target service flow.

[0127] When reporting the in-situ flow detection result of the target service flow to the controller, the network device may also report the target application-aware identifier of the target service flow. Therefore, the controller can further detect and analyze the transmission performance of the service flow by using a granularity indicated by at least one identifier in the target application-aware identifier, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved.

[0128] Optionally, the target application-aware identifier is encapsulated in the service packet. To be specific, the network device may directly obtain the target application-aware identifier from the service packet received by the network device, and the target application-aware identifier may indicate a user and/or an application to which the target service flow belongs.

[0129] The target application-aware identifier may be encapsulated by an upstream node (for example, an application-aware edge device) of the network device, or may be encapsulated by the application to which the target service flow belongs.

[0130] Optionally, if the in-situ flow detection information is IFIT information, the target application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information.

[0131] The target application-aware identifier is encapsulated in the IFIT information, so that the network device can synchronously obtain the target application-aware identifier when reading the IFIT information to perform in-situ flow detection.

[0132] Alternatively, the target application-aware identifier may be encapsulated in a destination address field, an HBH, a DOH, or an SRH of the service packet. For example, the target application-aware identifier may be encapsulated in a BSID field of the SRH field.

[0133] Optionally, the method may further include: receiving a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller, where the first application-aware identifier is generated by the controller based on a user requirement of a service flow; and if the target service flow is a service flow indicated by the first application-aware identifier, forwarding a service packet of the target service flow by using the first network service and based on the correspondence.

[0134] The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

[0135] Optionally, the method may further include: receiving an identifier generation rule sent by the controller; and generating a second application-aware identifier of the target service flow according to the identifier generation rule. The target application-aware identifier is the second application-aware identifier or the first application-aware identifier that is of the target service flow and that is sent by the controller.

[0136] In a scenario in which the application-aware identifier is not encapsulated in the received service packet, the network device may further generate a second application-aware identifier. The second application-aware identifier as a target application-aware identifier may be reported to the controller. Alternatively, if further receiving the first application-aware identifier that is of the target service flow and that is delivered by the controller, the network device may further determine that the second application-aware identifier matches the first application-aware identifier, and report the first application-aware identifier as the target application-aware identifier to the controller.

[0137] Optionally, the in-situ flow detection information is IFIT information. The method may further include: encapsulating the target application-aware identifier in a flow identifier field or a reserved field of the IFIT information, and forwarding the service packet in which the target application-aware identifier is encapsulated. Therefore, a downstream node of the network device can directly obtain, from the service packet, and report the target application-aware identifier.

[0138] Optionally, the method may further include: receiving a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow. Correspondingly, a process in which the network device sends the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller may include: sending the in-situ flow detection result and the target application-aware identifier of the target service flow to the controller based on the indication of the sending policy.

[0139] The controller may deliver a sending policy of a key service flow (including the target service flow) to the network device, so that the network device reports only an in-situ flow detection result of the key service flow, and does not need to report an in-situ flow detection result of a non-key service flow. Therefore, a reporting granularity of the in-situ flow detection result is flexibly adjusted, and data processing pressure of the controller is also effectively reduced.

[0140] Optionally, a process of sending the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller in a network may include: sending the in-situ flow detection result, the target application-aware identifier of the target service flow, and a corresponding in-situ flow detection flow identifier to the controller in the network.

[0141] The in-situ flow detection flow identifier may indicate a monitored data flow in the target service flow. Therefore, the controller may know a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, so that the controller analyzes transmission performance of at least one data flow included in the target service flow.

[0142] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier. The user identifier indicates a user to which the target service flow belongs, and the application identifier indicates an application to which the target service flow belongs.

[0143] Optionally, the target application-aware identifier may further include at least one of a flow identifier, an SLA level, or a service requirement. The service requirement may be a requirement for performance indicators such as a latency and a packet loss rate, and the flow identifier in the second application-aware identifier is also referred to as a session identifier (session ID).

[0144] According to a tenth aspect, a method for detecting performance of a service flow is provided, applied to a controller in a network, where the method includes: receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the in-situ flow detection result is obtained by the third network device by performing in-situ flow detection on a target service flow, and the target application-aware identifier is generated based on a user requirement of the target service flow; and analyzing transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0145] The third network device may be a node on an in-situ flow detection path of the target service flow, for example, may be an ingress node, a forwarding node (which may also be referred to as an intermediate node), or an egress node on an in-situ flow detection path.

[0146] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier. The method further includes: displaying a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by the at least one identifier in the target application-aware identifier.

[0147] The target application-aware identifier may include one or more identifiers, and the controller displays the performance indicator based on the granularity indicated by the at least one identifier. Therefore, refined display of the performance indicator can be implemented, and the display granularity can also be flexibly adjusted.

[0148] Optionally, before the receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, the method may further include: sending a sending policy of the target service flow to the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0149] Optionally, a process of receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device may include: receiving the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device. Correspondingly, a process of analyzing transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier may include: determining, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyzing, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0150] The controller may determine, based on the correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, the at least one monitored data flow included in the target service flow, and may further analyze the transmission performance of the target service flow based on the transmission performance of the at least one data flow.

[0151] Optionally, the method may further include: obtaining, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow; and sending the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow. The target application-aware identifier is the first application-aware identifier or a second application-aware identifier that is of the target service flow and that is generated by the network device.

[0152] The first network device may be a headend network device (also referred to as a head node) of the first network service. For example, the first network device is a head node of a forwarding path, or a head node of a network slice. It should be understood that, the first network device and the third network device may be a same network device, or may be different network devices.

[0153] Optionally, the method may further include: determining, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; determining that a network service required for transmitting the target service flow is a second network service; and sending a correspondence between the first application-aware identifier and the second network service to the first network device.

[0154] The controller can update, in time based on the detected transmission performance of the target service flow, the network service required for transmitting the target service flow. Therefore, it can be ensured that the updated network service can meet the transmission performance of the target service flow, so that reliable transmission of the target service flow is ensured.

[0155] Optionally, the method may further include: sending the first application-aware identifier of the target service flow to a second network device. The first application-aware identifier is used by the second network device to encapsulate the application-aware identifier of the target service flow in the service packet of the target service flow if the second network device determines that the received service flow is the target service flow.

[0156] The third network device may be an application-aware edge device in an APN. After the application-aware edge device encapsulates the application-aware identifier of the target service flow in the service packet of the target service flow, a downstream network device may determine, based on the application-aware identifier, the network service used to forward the target service flow, or may report the application-aware identifier of the target service flow when reporting an in-situ flow detection result of the target service flow.

[0157] Optionally, the method may further include: obtaining the user requirement of the target service flow through a northbound interface. For example, the controller may obtain, through the northbound interface of the controller, the user requirement that is of the target service flow and that is sent by a frontend.

[0158] Optionally, the user requirement of the target service flow includes one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

[0159] According to an eleventh aspect, a network device is provided. The network device includes:

> a detection module, configured to perform, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result; and
> a sending module, configured to send the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller in a network. The target application-aware identifier is generated based on a user requirement of the target service flow, and the in-situ flow detection result and the target application-aware identifier are used by the controller to analyze transmission performance of the target service flow.

[0160] Optionally, the target application-aware identifier is encapsulated in the service packet, and the target application-aware identifier may indicate a user and/or an application to which the target service flow belongs.

[0161] Optionally, if the in-situ flow detection information is IFIT information, the target application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information.

[0162] Optionally, the network device may further include:
a receiving module, configured to receive a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller, where the first application-aware identifier is generated by the controller based on a user requirement of a service flow.

[0163] The sending module is further configured to: if the target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence.

[0164] Optionally, the receiving module may be further configured to receive an identifier generation rule sent by the controller.

[0165] The network device may further include: a generation module, configured to generate a second application-aware identifier of the target service flow according to the identifier generation rule.

[0166] The target application-aware identifier is the second application-aware identifier or the first application-aware identifier that is of the target service flow and that is sent by the controller.

[0167] Optionally, the in-situ flow detection information is IFIT information. The network device may further include:
an encapsulation module, configured to encapsulate the target application-aware identifier in a flow identifier field or a reserved field of the IFIT information.

[0168] The sending module is further configured to forward the service packet in which the target application-aware identifier is encapsulated.

[0169] Optionally, the receiving module may be further configured to receive a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0170] The sending module is configured to send the in-situ flow detection result and the target application-aware identifier of the target service flow to the controller based on the indication of the sending policy.

[0171] Optionally, the sending module may be configured to send the in-situ flow detection result, the target application-aware identifier of the target service flow, and a corresponding in-situ flow detection flow identifier to the controller in the network.

[0172] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier.

[0173] According to a twelfth aspect, a controller is provided, where the controller includes:

a receiving module, configured to receive an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the in-situ flow detection result is obtained by the third network device by performing in-situ flow detection on a target service flow, and the target application-aware identifier is generated based on a user requirement of the target service flow; and
an analysis module, configured to analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0174] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier. The controller further includes:
a display module, configured to display a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

[0175] Optionally, the controller further includes:
a sending module, configured to send a sending policy of the target service flow to the third network device before the receiving module receives the in-situ flow detection result and the target application-aware identifier that are sent by the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow.

[0176] Optionally, the receiving module may be configured to receive the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by a third network device. Correspondingly, the analysis module may be configured to: determine, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyze, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0177] Optionally, the controller further includes:
a generation module, configured to obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow.

[0178] The sending module is further configured to send the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow.

[0179] The target application-aware identifier is the first application-aware identifier or a second application-aware identifier that is of the target service flow and that is generated by the network device.

[0180] Optionally, the generation module is further configured to: determine, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; and determine that a network service required for transmitting the target service flow is a second network service.

[0181] The sending module is further configured to send a correspondence between the first application-aware identifier and the second network service to the first network device.

[0182] Optionally, the sending module is further configured to send the first application-aware identifier of the target service flow to a second network device.

[0183] Optionally, the controller further includes:
an obtaining module, configured to obtain the user requirement of the target service flow through a northbound interface.

[0184] According to a thirteenth aspect, a controller is provided. The controller may include a memory, a processor, and a computer program that is stored in the memory and that can be run on the processor. When executing the computer program, the processor implements the method that is applied to the controller and that is provided in any one of the foregoing aspects.

[0185] According to a fourteenth aspect, a network device is provided. The network device may include a memory, a processor, and a computer program that is stored in the memory and that can be run on the processor. When executing the computer program, the processor implements the method that is applied to the network device and that is provided in any one of the foregoing aspects.

[0186] According to a fifteenth aspect, a network device is provided. The network device may include: a main control board and an interface board, and the interface board may be configured to implement the method that is applied to the network device and that is provided in any one of the foregoing aspects.

[0187] According to a sixteenth aspect, a network device is provided. The network device includes: a main control board and an interface board. The main control board includes: a first processor and a first memory. The interface board includes: a second processor, a second memory, and an interface card. The main control board is coupled to the interface board. The second memory may be configured to store program code, and the second processor is configured to invoke the program code in the second memory, to trigger the interface card to perform the following operations: receiving a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller in a network, where the first application-aware identifier is generated by the controller based on a user requirement of a service flow; and if the received target service flow is a service flow indicated by the first application-aware identifier, forwarding a service packet of the target service flow by using the first network service and based on the correspondence.

[0188] According to a seventeenth aspect, a network device is provided. The network device includes: a main control board and an interface board. The main control board includes: a first processor and a first memory. The interface board includes: a second processor, a second memory, and an interface card. The main control board is coupled to the interface board. The first memory may be configured to store program code, and the first processor is configured to invoke the program code in the first memory to perform the following operations: generating a first application-aware identifier of a target service flow based on a user requirement that is of the target service flow and that is sent by a controller; and encapsulating a target application-aware identifier in a service packet of the target service flow. The second memory may be configured to store program code, and the second processor is configured to invoke the program code in the second memory, to trigger the interface card to perform the following operations: forwarding the service packet in which the target application-aware identifier is encapsulated. The target application-aware identifier is the first application-aware identifier, or a second application-aware identifier matching the first application-aware identifier, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the target service flow.

[0189] Alternatively, the second processor is configured to invoke the program code in the second memory, to trigger the interface card to perform the following operations: receiving a first application-aware identifier sent by a controller, where the first application-aware identifier is generated based on a user requirement of a service flow, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the service flow; and if the received target service flow is a service flow indicated by the first application-aware identifier, encapsulating a target application-aware identifier in a service packet of the target service flow, and forwarding the service packet in which the target application-aware identifier is encapsulated. The target application-aware identifier is the first application-aware identifier, or a second application-aware identifier matching the first application-aware identifier.

[0190] According to an eighteenth aspect, a network device is provided. The network device includes: a main control board and an interface board. The main control board includes: a first processor and a first memory. The interface board includes: a second processor, a second memory, and an interface card. The main control board is coupled to the interface board. The first memory may be configured to store program code, and the first processor is configured to invoke the program code in the first memory to perform the following operations: performing, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result.

[0191] The second memory may be configured to store program code, and the second processor is configured to invoke the program code in the second memory, to trigger the interface card to perform the following operations: sending the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller in a network. The target application-aware identifier is generated based on a user requirement of the target service flow, and the in-situ flow detection result and the target application-aware identifier are used by the controller to analyze transmission performance of the target service flow.

[0192] According to a nineteenth aspect, a computer-readable storage medium is provided. The computer-readable storage medium stores instructions, and the instructions are executed by a processor to implement the method provided in any one of the foregoing aspects.

[0193] According to a twentieth aspect, a computer program product including instructions is provided. When the computer program product runs on a computer, the computer is enabled to perform the method provided in any one of the foregoing aspects.

[0194] According to a twenty-first aspect, a communication network is provided, where the communication network may include: a controller and at least one network device. The controller may implement the method that is applied to the controller and that is provided in any one of the foregoing aspects, and the network device may implement the method that is applied to the network device and that is provided in any one of the foregoing aspects.

[0195] According to a twenty-second aspect, a chip is provided. The chip may be configured to implement the method provided in any one of the foregoing aspects.

[0196] In conclusion, this application provides a packet forwarding method and apparatus, and a communication network, where a controller may obtain a correspondence between an application-aware identifier of a service flow and a network service required for transmitting the service flow, and deliver the correspondence to a network device. Further, when identifying the service flow as a service flow indicated by the application-aware identifier, the network device may directly forward a packet of the service flow by using the corresponding network service. The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

BRIEF DESCRIPTION OF DRAWINGS

[0197]

FIG. 1 is a schematic diagram of a structure of a communication network according to an embodiment of this application;
FIG. 2 is a flowchart of a packet forwarding method according to an embodiment of this application;
FIG. 3 is a schematic diagram of a data structure of an application-aware identifier according to an embodiment of this application;
FIG. 4 is a flowchart of another packet forwarding method according to an embodiment of this application;
FIG. 5 is a flowchart of a method for detecting performance of a service flow according to an embodiment of this application;
FIG. 6 is a flowchart of still another packet forwarding method according to an embodiment of this application;
FIG. 7 is a schematic diagram of a structure of another communication network according to an embodiment of this application;
FIG. 8 is a schematic diagram of a data structure of another application-aware identifier according to an embodiment of this application;
FIG. 9 is a schematic diagram of a data structure of still another application-aware identifier according to an embodiment of this application;
FIG. 10 is a flowchart of yet another packet forwarding method according to an embodiment of this application;
FIG. 11 is a flowchart of another method for detecting performance of a service flow according to an embodiment of this application;
FIG. 12 is a schematic diagram of a structure of IFIT information according to an embodiment of this application;
FIG. 13 is a schematic diagram of a structure of a controller according to an embodiment of this application;
FIG. 14 is a schematic diagram of a structure of another controller according to an embodiment of this application;
FIG. 15 is a schematic diagram of a structure of a network device according to an embodiment of this application;
FIG. 16 is a schematic diagram of a structure of another network device according to an embodiment of this application;
FIG. 17 is a schematic diagram of a structure of a packet forwarding apparatus according to an embodiment of this application;
FIG. 18 is a schematic diagram of a structure of another packet forwarding apparatus according to an embodiment of this application;
FIG. 19 is a schematic diagram of a structure of still another packet forwarding apparatus according to an embodiment of this application;
FIG. 20 is a schematic diagram of a structure of still another network device according to an embodiment of this application;
FIG. 21 is a schematic diagram of a structure of yet another network device according to an embodiment of this application;
FIG. 22 is a schematic diagram of a structure of yet another network device according to an embodiment of this application;
FIG. 23 is a schematic diagram of a structure of still another controller according to an embodiment of this application;
FIG. 24 is a schematic diagram of a structure of yet another packet forwarding apparatus according to an embodiment of this application; and
FIG. 25 is a schematic diagram of a structure of yet another network device according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[0198] With reference to the accompanying drawings, the following describes in detail a packet forwarding method and apparatus, and a communication network that are provided in embodiments of this application.

[0199] FIG. 1 is a schematic diagram of a structure of a communication network according to an embodiment of this application. As shown in FIG. 1, the communication network may include a controller 01 and a plurality of network devices. For example, FIG. 1 schematically shows a total of five network devices 02a to 02e. A communication connection is established between the controller 01 and at least one network device, and a communication connection is established between the plurality of network devices.

[0200] The controller 01 may be a network controller, for example, may be a software-defined networking (software-defined networking, SDN) controller, a network control engine (network control engine, NCE), or a path computation element server (path computation element server, PCE server). In addition, the controller 01 may be a server, a server cluster including several servers, or a cloud computing service center. Each network device may be a device that has a packet forwarding function, such as a router or a switch, and each network device may also be referred to as a node.

[0201] Optionally, the plurality of network devices may include a provider (provider, P) device, a provider edge (provider edge, PE) device, a broadband remote access server (broadband remote access server, BRAS), customer premises equipment (customer premises equipment, CPE), and the like.

[0202] Refer to FIG. 1. The at least one network device (for example, the PE device or the CPE) in the communication network may be further connected to a user terminal 03, and is configured to provide a network access service for the user terminal 03. The user terminal 03 may also be referred to as a host or user equipment. An application (application, APP) is installed in the user terminal 03, and the plurality of network devices may forward a service flow of the APP.

[0203] It may be understood that the communication network provided in this embodiment of this application may be an APN. For example, the APN may be a network based on internet protocol version 6 (Internet protocol version 6, IPv6), and is also referred to as an APN 6. Alternatively, the APN may be a network based on SRv6, a multi-protocol label switching (multi-protocol label switching, MPLS) technology, or a virtual extensible local area network (virtual extensible local area network, VXLAN). SRv6 is an IPv6-based segment routing (segment routing, SR) forwarding technology.

[0204] An embodiment of this application provides a packet forwarding method. The method may be applied to the communication network shown in FIG. 1. Refer to FIG. 2. The method includes the following steps.

[0205] Step 101: A controller obtains, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow.

[0206] The user requirement of the target service flow is a requirement of the target service flow for performance of the network service. For example, the user requirement may include one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance. The performance indicator of the transmission performance may include a latency, a bandwidth, a packet loss rate, and the like. In addition, the user requirement of the target service flow may further include information about a user and/or an application to which the target service flow belongs.

[0207] The controller may generate the first application-aware identifier of the target service flow based on the user requirement of the target service flow. FIG. 3 is a schematic diagram of a structure of an application-aware identifier according to an embodiment of this application. As shown in FIG. 3, the first application-aware identifier includes at least one of a user identifier (user ID) and an application identifier (APP ID). The user identifier is used to identify a user to which the target service flow belongs. The application identifier is used to identify an application to which the target service flow belongs. It should be understood that the user to which the target service flow belongs may be a user, or may be a user group. The application to which the target service flow belongs may be an application, or may be an application group.

[0208] Still refer to FIG. 3. The first application-aware identifier may further include at least one of a flow identifier (flow ID) and an SLA level. The flow identifier (also referred to as a session ID) is used to identify a specified flow (namely, a specific session) in the application to which the target service flow belongs. The SLA level is used to identify a service level of the user to which the target service flow belongs. The service level may include levels such as gold, silver, and bronze, or the service level may be further distinguished by using different colors (colors).

[0209] The controller may further obtain, through calculation based on a user requirement of the target service flow, a first network service that can meet the user requirement. The first network service may include a network slice and/or a forwarding path. For example, the first network service may include a specified network slice or a specified forwarding path in the user requirement. The forwarding path may be an SRv6 path.

[0210] Step 102: The controller sends the correspondence to the first network device.

[0211] The correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow. The first network device may be a headend network device (also referred to as a head node) of the first network service. For example, the first network device is a head node of a forwarding path, or a head node of a network slice.

[0212] Optionally, the first application-aware identifier and an identifier of the first network service corresponding to the first application-aware identifier are recorded in the correspondence. If the first network service includes the network slice, the identifier of the first network service includes an identifier of the network slice. If the first network service includes the forwarding path, the identifier of the first network service includes an identifier of the forwarding path. The identifier of the forwarding path may be a BSID of the forwarding path, or may be a BSID of an SR policy to which the forwarding path belongs.

[0213] Step 103: If the target service flow received by the first network device is a service flow indicated by the first application-aware identifier, forward the service packet of the target service flow by using the first network service and based on the correspondence.

[0214] The first network device may identify the service flow received by the first network device. If identifying the target service flow received by the first network device as the service flow indicated by the first application-aware identifier, the first network device may forward the service packet of the target service flow by using the first network service and based on the correspondence delivered by the controller. For example, assuming that the first network service includes the SRv6 path, the first network device may forward the service packet of the target service flow through the SRv6 path.

[0215] In a possible example, the first network device may identify the service flow by using an application-aware identifier encapsulated in the service packet of the target service flow. If detecting that the application-aware identifier encapsulated in the service packet of the target service flow matches the first application-aware identifier, the first network device may determine that the target service flow is the service flow indicated by the first application-aware identifier.

[0216] In another possible example, the first network device may further identify, in a manner of parsing the packet or analyze a traffic feature, whether the target service flow is the service flow indicated by the first application-aware identifier. For example, the first network device may identify the target service flow by analyzing 4-tuple information, 5-tuple information, or 7-tuple information of the service packet. Alternatively, the first network device may further analyze the service packet of the target service flow by using a deep packet inspection (deep packet inspection, DPI) technology, to identify whether the target service flow is the service flow indicated by the first application-aware identifier. Alternatively, the first network device may further analyze the traffic feature of the target service flow by using an artificial intelligence (artificial intelligence, AI) model, to identify whether the target service flow is the service flow indicated by the first application-aware identifier. The AI model may be delivered by the controller to the first network device.

[0217] It may be understood that, in this embodiment of this application, the application-aware identifier of the service flow may also be referred to as an APN identifier or an APN ID.

[0218] In conclusion, this embodiment of this application provides a packet forwarding method, where a controller may obtain a correspondence between an application-aware identifier of a service flow and a network service required for transmitting the service flow, and deliver the correspondence to a network device. Further, when identifying the service flow as a service flow indicated by the application-aware identifier, the network device may directly forward a packet of the service flow by using the corresponding network service. The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

[0219] An embodiment of this application provides another packet forwarding method. The method may be applied to the communication network shown in FIG. 1, and may be applied to a controller or any network device in the communication network. Refer to FIG. 4. The method includes the following steps.

[0220] Step 201: Generate a first application-aware identifier of a target service flow based on a user requirement of the target service flow, where the first application-aware identifier is used by a network device to encapsulate a target application-aware identifier in a service packet of the target service flow, and the first application-aware identifier corresponds to a first network service.

[0221] The first network service meets the user requirement of the target service flow. The target application-aware identifier may be the first application-aware identifier, or a second application-aware identifier matching the first application-aware identifier. In this embodiment of this application, the controller may generate the first application-aware identifier of the target service flow based on the user requirement that is of the target service flow and that is obtained by the controller. Alternatively, the second network device may generate the first application-aware identifier of the target service flow based on the user requirement that is of the target service flow and that is delivered by the controller.

[0222] The user requirement of the target service flow is a requirement of the target service flow for performance of the network service, and the user requirement of the target service flow may further include information about a user and/or an application to which the target service flow belongs. The first network service may include a network slice and/or a forwarding path. For a structure of the first application-aware identifier, refer to FIG. 3.

[0223] Step 202: Send the first application-aware identifier, where the first application-aware identifier is used by the network device to forward the service packet of the target service flow by using the first network service.

[0224] If the first application-aware identifier is generated by the controller, the controller may send the first application-aware identifier to a second network device. The second network device is an application-aware edge device. If determining that the received target service flow is a service flow indicated by the first application-aware identifier, the second network device may encapsulate the target application-aware identifier in the service packet of the target service flow. The target application-aware identifier may be the first application-aware identifier, or may be a second application-aware identifier that is of a target service flow and that is generated by the second network device, and the second application-aware identifier matches the first application-aware identifier. Therefore, a downstream network device of the second network device may determine, based on the target application-aware identifier, a first network service used to forward the target service flow, and further forward the service packet of the target service flow by using the first network service.

[0225] If the first application-aware identifier is generated by the second network device, the second network device may encapsulate the first application-aware identifier in the service packet of the target service flow, and forward, to a downstream network device, the service packet in which the first application-aware identifier is encapsulated. The downstream network device may further determine, based on the first application-aware identifier, a first network service used to forward the target service flow, and forward the service packet of the target service flow by using the first network service.

[0226] In conclusion, this embodiment of this application provides a packet forwarding method. In the method, a first application-aware identifier can be generated based on a user requirement of a target service flow. The first application-aware identifier corresponds to a first network service, and is used by a network device to encapsulate a target application-aware identifier in a service packet of the target service flow. Therefore, it can be ensured that the network device that receives the service packet can forward the service packet by using the corresponding first network service, so that flexibility of forwarding the service packet is effectively improved.

[0227] An embodiment of this application provides a method for detecting performance of a service flow. The method may be applied to the communication network shown in FIG. 1. Refer to FIG. 5. The method includes the following steps.

[0228] Step 301: A third network device performs, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result.

[0229] In this embodiment of this application, the third network device may be a node on a forwarding path of the target service flow, and the third network device may be an ingress (ingress) node, a transit (transit) node, or an egress (egress) node on an in-situ flow detection path of the target service flow. The in-situ flow detection result may include a measurement result of a performance indicator such as a latency and/or a packet loss rate of the target service flow.

[0230] It may be understood that the in-situ flow detection information may be encapsulated in the service packet by an ingress node on the in-situ flow detection path of the target service flow, and the ingress node may be an upstream node of the third network device, or may be the third network device. If the third network device is the ingress node, the third network device may encapsulate the in-situ flow detection information in the service packet of the target service flow, and may perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain the in-situ flow detection result.

[0231] Step 302: The third network device sends the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller in the network.

[0232] The target application-aware identifier is generated based on a user requirement of the target service flow, and the in-situ flow detection result and the target application-aware identifier are used by the controller to analyze transmission performance of the target service flow. The user requirement of the target service flow is a requirement of the target service flow for the performance of the network service. For a structure of the target application-aware identifier, refer to FIG. 3.

[0233] In a possible implementation, the target application-aware identifier is encapsulated in the service packet that is of the target service flow and that is received by the third network device. The target application-aware identifier may be encapsulated in the service packet by the upstream node (for example, an application-aware edge device) of the third network device or an application to which the target service flow belongs. In addition, the target application-aware identifier may be a second application-aware identifier generated by the upstream node or the application to which the target service flow belongs, or may be a first application-aware identifier delivered by the controller.

[0234] In another possible implementation, the target application-aware identifier of the target service flow is not encapsulated in the service packet that is of the target service flow and that is received by the third network device. In this implementation, the third network device may generate the second application-aware identifier of the target service flow based on an identifier generation rule delivered by the controller. Correspondingly, the target application-aware identifier is the second application-aware identifier generated by the third network device.

[0235] Step 303: The controller analyzes the transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0236] After receiving the in-situ flow detection result and the target application-aware identifier that are sent by the third network device, the controller can analyze the transmission performance of the target service flow by using a granularity indicated by at least one identifier in the target application-aware identifier. The transmission performance may be represented by using a performance indicator such as a packet loss rate and/or a latency.

[0237] It may be understood that the controller may receive in-situ flow detection results and application-aware identifiers that are of different service flows and that are reported by different network devices, and the controller may determine an in-situ flow detection result of a same service flow based on the application-aware identifier, and may further analyze transmission performance of the service flow based on one or more in-situ flow detection results of the same service flow.

[0238] In conclusion, this embodiment of this application provides a method for detecting performance of a service flow. When reporting an in-situ flow detection result of a target service flow to the controller, the network device may also report a target application-aware identifier of the target service flow. Further, the controller can detect and analyze transmission performance of the service flow by using a granularity indicated by at least one identifier in the target application-aware identifier, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved.

[0239] FIG. 6 is a flowchart of still another packet forwarding method according to an embodiment of this application. The method may be applied to the communication network shown in FIG. 1. Refer to FIG. 6. The method includes the following steps.

[0240] Step 401: A controller obtains a user requirement of a target service flow.

[0241] The user requirement of the target service flow is a requirement of the target service flow for performance of a network service. For example, the user requirement may include one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance. The performance indicator of the transmission performance may include a latency, a bandwidth, a packet loss rate, and the like. In addition, the user requirement of the target service flow may further include information about a user and/or an application to which the target service flow belongs.

[0242] In this embodiment of this application, the controller may obtain the user requirement of the target service flow through a northbound interface (northbound interface) of the controller. For example, the northbound interface of the controller may be connected to another device, so that the controller obtains the user requirement that is of the target service flow and that is sent by the device. Specifically, the device connected to the northbound interface of the controller includes but is not limited to a frontend (frontend), a portal (portal), an orchestrator, an operation support system (operation support system, OSS), or a business support system (business support system, BSS).

[0243] Step 402: The controller obtains, based on the user requirement, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow.

[0244] The controller may generate the first application-aware identifier of the target service flow based on the user requirement of the target service flow. As shown in FIG. 3, the first application-aware identifier includes at least one of a user identifier and an application identifier. The user identifier is used to identify a user to which the target service flow belongs. The application identifier is used to identify an application to which the target service flow belongs. For example, assuming that the application to which the target service flow belongs is an enterprise application, the user identifier may be an identifier of an enterprise.

[0245] Still refer to FIG. 3. The first application-aware identifier may further include at least one of a flow identifier and an SLA level. The flow identifier is used to identify a specified data flow in the application to which the target service flow belongs. The SLA level is used to identify a service level of the user to which the target service flow belongs. The service level may include levels such as gold, silver, and bronze, or the service level may be further distinguished by using different colors.

[0246] The controller may further obtain, through calculation based on the user requirement of the target service flow, the first network service that can meet the user requirement, to obtain a correspondence between the first application-aware identifier and the first network service. The first network service may include a network slice and/or a forwarding path.

[0247] It may be understood that the first application-aware identifier and an identifier of the first network service corresponding to the first application-aware identifier may be recorded in the correspondence. In other words, the correspondence may be a correspondence between the first application-aware identifier and the identifier of the first network service. If the first network service includes the network slice, the identifier of the first network service may include an identifier of the network slice. If the first network service includes the forwarding path, the identifier of the first network service may include an identifier of the forwarding path. The forwarding path may be an SRv6 path, and the identifier of the forwarding path may be a BSID of the forwarding path, or may be a BSID of an SR policy to which the forwarding path belongs.

[0248] Step 403: The controller separately sends the correspondence to the first network device and a second network device.

[0249] The first network device may be a headend network device (also referred to as a head node) of the first network service. For example, the first network device is a head node of a forwarding path, or a head node of a network slice. The correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow.

[0250] The second network device may be an application-aware edge device (App-aware edge device) in an ANP network, and the second network device may be a BRAS, a PE device, a CPE, an egress gateway (for example, an egress gateway of a campus), or the like. The first application-aware identifier in the correspondence is used by the second network device to: encapsulate, if the second network device determines that the received service flow is the target service flow, an application-aware identifier of the target service flow in the service packet of the target service flow, for example, encapsulate the first application-aware identifier.

[0251] For example, refer to FIG. 1. It is assumed that a network device 02a is the application-aware edge device (namely, the second network device). If a network device 02b is a headend network device (namely, the first network device) of the first network service, the controller 01 may separately deliver the correspondence to the network device 02a and the network device 02b. The correspondence delivered by the controller 01 may be shown in Table 1. Refer to Table 1. In the correspondence, an identifier of a first network service corresponding to a target service flow whose first application-aware identifier is an APN ID 1 is a BSID 1. That is, the first network service allocated by the controller 01 to the target service flow is an SRv6 path indicated by the BSID 1. An identifier of a first network service corresponding to a target service flow whose first application-aware identifier is an APN ID 3 is a slice-ID 1. That is, the first network service allocated by the controller 01 to the target service flow is a network slice indicated by the slice-ID 1.

Table 1

First application-aware identifier	Identifier of first network service
APN ID 1	BSID 1
APN ID 2	BSID 2
APN ID 3	Slice-ID 1

[0252] It may be understood that the first network device and the second network device may be a same network device. That is, the application-aware edge device is the headend network device of the first network service. In this scenario, the controller may deliver the correspondence to only one network device. For example, refer to FIG. 7. It is assumed that a network device 02a is the application-aware edge device (namely, the second network device). If the network device 02a is also the headend network device (namely, the first network device) of the first network service, the controller 01 may deliver the correspondence to only the network device 02a.

[0253] It may be further understood that, in a scenario in which the first network device and the second network device are different network devices, the controller may deliver the first application-aware identifier to only the second network device (for example, the network device 02a shown in FIG. 1), and does not need to deliver the correspondence.

[0254] Step 404: The controller sends an identifier generation rule to the second network device.

[0255] The identifier generation rule may be a rule for generating an application-aware identifier of a service flow based on feature information of the service flow. The identifier generation rule is used by the second network device to generate a second application-aware identifier of the target service flow, and the second application-aware identifier is used to match the first application-aware identifier generated by the controller, so that the second network device determines whether the target service flow received by the second network device is a service flow indicated by the first application-aware identifier.

[0256] For example, as shown in FIG. 1, the controller 01 may deliver the identifier generation rule to the network device 02a.

[0257] Step 405: The second network device generates the second application-aware identifier of the target service flow according to the identifier generation rule.

[0258] After receiving the identifier generation rule delivered by the controller, the second network device may generate, according to the identifier generation rule, the application-aware identifier for the service flow received by the second network device. In this embodiment of this application, the second network device may obtain feature information of the target service flow received by the second network device, and process the feature information according to the identifier generation rule, to generate the second application-aware identifier of the target service flow. The feature information may include information such as 4-tuple information, 5-tuple information, or 7-tuple information of the target service flow, or may further include traffic feature information (for example, a packet interval) of the target service flow, or may further include information obtained based on a DPI technology or an application identification technology.

[0259] For example, assuming that the identifier generation rule is an AI model, the second network device may input the traffic feature information of the target service flow into the AI model, to obtain the second application-aware identifier that is of the target service flow and that is output by the AI model.

[0260] It may be understood that the second application-aware identifier has a same structure as the first application-aware identifier. If the first application-aware identifier includes an application identifier, the second network device may identify, based on the application identification technology, an application to which the target service flow belongs, and may further generate, according to the identifier generation rule, the application identifier of the application to which the target service flow belongs. If the first application-aware identifier includes a user identifier, the second network device may determine, based on information such as a virtual local area network (virtual local area network, VLAN) or an interface of the target service flow, a user to which the target service flow belongs, and may further generate, according to the identifier generation rule, the user identifier of the user to which the target service flow belongs.

[0261] Step 406: If the second application-aware identifier matches the first application-aware identifier, the second network device encapsulates a target application-aware identifier in the service packet of the target service flow.

[0262] In this embodiment of this application, if detecting that the second application-aware identifier that is of the target service flow and that is generated by the second network device matches the first application-aware identifier delivered by the controller, the second network device may determine that the target service flow is the service flow indicated by the first application-aware identifier. Because the second application-aware identifier is generated by the second network device according to the identifier generation rule delivered by the controller, it can be ensured that the second application-aware identifier accurately matches the first application-aware identifier delivered by the controller, that is, reliability of identifying the target service flow by the second network device is ensured.

[0263] As the application-aware edge device, the second network device may further encapsulate the target application-aware identifier in the service packet of the target service flow. The target application-aware identifier may be the first application-aware identifier delivered by the controller, or may be the second application-aware identifier generated by the second network device.

[0264] Optionally, the second network device may encapsulate the target application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet. For example, the SRH includes a BSID field, and the second network device may encapsulate the target application-aware identifier in the BSID field.

[0265] Alternatively, if the service packet received by the second network device includes in-situ flow detection information, the second network device may alternatively encapsulate the target application-aware identifier in the in-situ flow detection information. For example, if the in-situ flow detection information is IFIT information, the second network device may encapsulate the target application-aware identifier in a flow identifier field or a reserved field of the IFIT information.

[0266] For example, as shown in FIG. 1, the network device 02a may generate a second application-aware identifier of the target service flow according to the identifier generation rule delivered by the controller 01. It is assumed that the second application-aware identifier generated by the network device 02a is an APN ID 1. Because the second application-aware identifier is the same as the first application-aware identifier APN ID 1 in the correspondence shown in Table 1, the network device 02a may encapsulate the APN ID 1 in the service packet of the target service flow. For example, the network device 02a may encapsulate the APN ID 1 in a BSID field of the service packet.

[0267] In a possible example, a structure of the target application-aware identifier encapsulated in the service packet may be shown in FIG. 3. Refer to FIG. 3. The target application-aware identifier may include: an SLA level, an application identifier, a user identifier, and a flow identifier.

[0268] In another possible example, a structure of the target application-aware identifier encapsulated in the service packet may be shown in FIG. 8. Refer to FIG. 8. The target application-aware identifier may include: an SLA level, an application identifier, a user identifier, a flow identifier, and an arguments (arguments) field. The arguments field may indicate a service requirement of the target service flow, for example, may indicate an upper limit of a latency and/or an upper limit of a packet loss rate of the target service flow.

[0269] In still another possible example, the target application-aware identifier may be encapsulated in an arguments field of a segment identifier (segment ID, SID) in an SRv6 packet. As shown in FIG. 9, a SID in an SRv6 packet includes: a locator address (locator address) field, a function identifier (function ID) field, and an arguments field. The target application-aware identifier shown in FIG. 3 or FIG. 8 may be encapsulated in the arguments field.

[0270] For related explanations of the application-aware identifier, refer to a draft: draft-li-6man-app-aware-ipv6-network-03. Related content in the draft may be incorporated in embodiments of this application by reference.

[0271] It may be understood that, that the second application-aware identifier generated by the second network device matches the first application-aware identifier delivered by the controller may mean that the second application-aware identifier is the same as the first application-aware identifier, or may mean that the second application-aware identifier is different from the first application-aware identifier, but there is a specific correspondence between the two.

[0272] The correspondence between the application-aware identifiers may be delivered by the controller. That is, the controller may deliver the identifier generation rule and the correspondence between the application-aware identifiers, to ensure that the application-aware identifiers generated by the controller and the network device are synchronized with each other. For example, the controller may deliver a correspondence between the first application-aware identifier and another application-aware identifier matching the first application-aware identifier to the second network device, and the second network device may determine, based on the correspondence delivered by the controller, whether the second application-aware identifier generated by the second network device matches the first application-aware identifier.

[0273] It may be further understood that, if the second application-aware identifier generated by the second network device is different from the first application-aware identifier, the second network device may further report the correspondence between the second application-aware identifier and the first application-aware identifier to the controller, so that the controller can also know the application-aware identifier that is of the target service flow and that is generated by the network device. For example, for a service flow of a video conference APP, assuming that the first application-aware identifier generated by the controller is an APN 11, and the second application-aware identifier generated by the second network device is an APN 12, the second network device may report a correspondence between the APN 12 and the APN 11 to the controller.

[0274] Step 407: The second network device forwards the service packet of the target service flow to the first network device.

[0275] The second network device may forward, to the first network device, the service packet in which the target application-aware identifier is encapsulated. The first network device may be a headend network device of the first network service.

[0276] For example, refer to FIG. 1. The second network device 02a may forward, to the first network device 02b, the service packet in which the target application-aware identifier is encapsulated.

[0277] Step 408: If determining that the received target service flow is the service flow indicated by the first application-aware identifier, the first network device forwards the service packet of the target service flow by using the first network service and based on the correspondence.

[0278] The first network device may identify, based on the application-aware identifier encapsulated in the service packet of the service flow, the service flow received by the first network device. If detecting that the target application-aware identifier in the service packet of the target service flow matches the first application-aware identifier, the first network device may determine that the target service flow is the service flow indicated by the first application-aware identifier. Further, the first network device may forward the service packet of the target service flow by using the first network service and based on the correspondence delivered by the controller.

[0279] For example, refer to FIG. 1. Assuming that the target application-aware identifier that is encapsulated in the service packet of the target service flow and that is received by the network device 02b (namely, the first network device) is the APN ID 1, the network device 02b may determine, based on the correspondence shown in Table 1, that the first network service allocated by the controller 01 to the target service flow is the SRv6 path indicated by the BSID 1. Therefore, the network device 02b may forward the service packet of the target service flow through the SRv6 path indicated by the BSID 1.

[0280] It may be understood that in a scenario in which the second network device and the first network device are different network devices, the controller may deliver the correspondence to only the first network device in step 403, and may delete step 404 to step 406 based on a situation. To be specific, the second network device does not need to identify the target service flow and encapsulate the target application-aware identifier. Correspondingly, the first network device may further identity, in a manner of parsing the packet or analyze a traffic feature, whether the target service flow is the service flow indicated by the first application-aware identifier. Alternatively, when sending the target service flow, the application to which the target service flow belongs may encapsulate the application-aware identifier of the target service flow in the service packet, and the first network device may identify, based on the application-aware identifier encapsulated by the application to which the target service flow belongs, whether the target service flow received by the first network device is the service flow indicated by the first application-aware identifier.

[0281] It may be further understood that, in a scenario in which the second network device and the first network device are a same network device, step 407 may be deleted. Alternatively, step 404 and step 403 may be performed synchronously. To be specific, the controller may deliver the identifier generation rule while delivering the correspondence to the first network device (or the second network device). Alternatively, step 405 may be deleted based on a situation. To be specific, the first network device (or the second network device) may not need to generate the second application-aware identifier, but may identify, in a manner of parsing the packet or analyzing the traffic feature, whether the received service flow is the service flow indicated by the first application-aware identifier. Alternatively, step 406 may be deleted based on a situation. To be specific, the first network device (or the second network device) may not need to encapsulate the target application-aware identifier in the service packet of the target service flow.

[0282] In conclusion, this embodiment of this application provides a packet forwarding method, where a controller may obtain a correspondence between an application-aware identifier of a service flow and a network service required for transmitting the service flow, and deliver the correspondence to a network device. Further, when identifying the service flow as a service flow indicated by the application-aware identifier, the network device may directly forward a packet of the service flow by using the corresponding network service. The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

[0283] FIG. 10 is a flowchart of yet another packet forwarding method according to an embodiment of this application. The method may be applied to the communication network shown in FIG. 1 or FIG. 7. Refer to FIG. 10. The method includes the following steps.

[0284] Step 501: A controller obtains a user requirement of a target service flow.

[0285] In this embodiment of this application, the controller may obtain the user requirement of the target service flow through a northbound interface. For example, the northbound interface of the controller may be connected to a frontend, so that the controller may obtain the user requirement that is of the target service flow and that is sent by the frontend. For an implementation process of step 501, refer to the related descriptions of step 401.

[0286] Step 502: The controller generates a first application-aware identifier of the target service flow based on the user requirement.

[0287] The first application-aware identifier is used to be encapsulated in a service packet of the target service flow, and the first application-aware identifier corresponds to a first network service, for example, corresponds to an identifier of the first network service. The first network service meets the user requirement of the target service flow. The first application-aware identifier includes at least one of a user identifier and an application identifier, and may further include at least one of a flow identifier and an SLA level. The first network service may include a forwarding path and/or a network slice. For an implementation process of step 502, refer to the related descriptions of step 402.

[0288] Step 503: The controller sends the first application-aware identifier to a second network device.

[0289] The second network device may be an application-aware edge device in an ANP network, and the second network device may be a BRAS, a PE device, a CPE, an egress gateway (for example, an egress gateway of a campus), or the like. The first application-aware identifier indicates a user and/or an application to which the target service flow belongs, and the first application-aware identifier is used by the second network device to encapsulate the first application-aware identifier in the service packet of the target service flow.

[0290] Step 504: The controller determines, based on the user requirement, the first network service required for transmitting the target service flow.

[0291] The controller may obtain, through calculation based on the user requirement of the target service flow, the first network service that can meet the user requirement. The first network service may include the network slice and/or the forwarding path. For an implementation process of step 504, refer to the related descriptions of step 402.

[0292] Step 505: The controller sends a correspondence between the first application-aware identifier and the first network service to a first network device.

[0293] The first network device may be a headend network device of the first network service. The correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward the service packet of the target service flow.

[0294] It may be understood that the first application-aware identifier and the identifier of the first network service corresponding to the first application-aware identifier may be recorded in the correspondence. In other words, the correspondence may be a correspondence between the first application-aware identifier and the identifier of the first network service. If the first network service includes the network slice, the identifier of the first network service may include an identifier of the network slice. If the first network service includes the forwarding path, the identifier of the first network service may include an identifier of the forwarding path. The forwarding path may be an SRv6 path, and the identifier of the forwarding path may be a BSID of the forwarding path, or may be a BSID of an SR policy to which the forwarding path belongs.

[0295] Step 506: If a target service flow received by the second network device is a service flow indicated by the first application-aware identifier, encapsulate a target application-aware identifier in the service packet of the target service flow.

[0296] The second network device may identify the service flow received by the second network device. If identifying the target service flow received by the second network device as the service flow indicated by the first application-aware identifier, the second network device may encapsulate the target application-aware identifier in the service packet of the target service flow. Therefore, a downstream network device (for example, the first network device) may determine, based on the target application-aware identifier, the first network service used to forward the service packet of the target service flow, and/or may also report the target application-aware identifier when reporting an in-situ flow detection result for the target service flow to the controller.

[0297] The target application-aware identifier may be the first application-aware identifier delivered by the controller, or may be a second application-aware identifier that is of the target service flow and that is generated by the second network device. For a process in which the second network device encapsulates the target application-aware identifier in the service packet, refer to the related descriptions of step 406. Details are not described herein again.

[0298] In a possible example, the second network device may identify, in a manner of parsing the packet or analyze a traffic feature, whether the service flow is the service flow indicated by the first application-aware identifier. For example, the second network device may identify, by analyzing 4-tuple information, 5-tuple information, or 7-tuple information of the service packet, whether the service flow is the service flow indicated by the first application-aware identifier. Alternatively, the second network device may further analyze the service packet of the service flow by using a DPI technology, to identify whether the service flow is the service flow indicated by the first application-aware identifier. Alternatively, the second network device may further analyze the traffic feature of the service flow by using an AI model, to identify whether the service flow is the service flow indicated by the first application-aware identifier.

[0299] In another possible example, the controller may synchronously deliver an identifier generation rule in step 503, and the second network device may generate the second application-aware identifier of the target service flow according to the identifier generation rule. If the second application-aware identifier matches the first application-aware identifier, the second network device may determine that the target service flow received by the second network device is the service flow indicated by the first application-aware identifier. For a process in which the second network device generates the second application-aware identifier according to the identifier generation rule delivered by the controller, refer to the related descriptions of step 404 and step 405. Details are not described herein again.

[0300] Step 507: The second network device forwards, to the first network device, the service packet in which the target application-aware identifier is encapsulated.

[0301] For an implementation process of step 507, refer to the related descriptions of step 407.

[0302] Step 508: If determining that the received target service flow is the service flow indicated by the first application-aware identifier, the first network device forwards the service packet of the target service flow by using the first network service and based on the correspondence.

[0303] If detecting that the target application-aware identifier is encapsulated in the service packet of the target service flow, the first network device may forward the service packet of the target service flow by using the first network service corresponding to the target application-aware identifier and based on the correspondence delivered by the controller. For an implementation process of step 508, refer to the related descriptions of step 408.

[0304] It may be understood that, after step 501, the controller may further send, to the second network device, the user requirement that is of the target service flow and that is obtained by the controller. Correspondingly, the second network device may generate the first application-aware identifier of the target service flow based on the user requirement sent by the controller. In other words, step 503 may be deleted, and the second network device may perform step 502. For example, both the controller and the second network device may perform step 502.

[0305] In conclusion, this embodiment of this application provides a packet forwarding method. A controller or a second network device can generate a first application-aware identifier of a target service flow based on a user requirement of the target service flow. The first application-aware identifier corresponds to a first network service, and is used by the network device to encapsulate a target application-aware identifier in a service packet of the target service flow. Therefore, it can be ensured that the network device that receives the service packet can forward the service packet by using the corresponding first network service, so that flexibility of forwarding the service packet is effectively improved. In addition, according to the method provided in this embodiment of this application, the controller or the second network device may alternatively generate an application-aware identifier of the service flow. Therefore, manners of generating the application-aware identifier are effectively enriched.

[0306] FIG. 11 is a flowchart of another method for detecting performance of a service flow according to an embodiment of this application. As shown in FIG. 11, the method includes the following steps.

[0307] Step 601: A controller obtains a user requirement of a target service flow.

[0308] Step 602: The controller obtains, based on the user requirement, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow.

[0309] Step 603: The controller separately sends the correspondence to the first network device and a third network device.

[0310] For an implementation process of step 601 to step 603, refer to the related descriptions of step 401 to step 403, or refer to the related descriptions of step 501, step 502, step 504, and step 505.

[0311] Step 604: The controller sends a sending policy of the target service flow to the first network device and/or the third network device.

[0312] The sending policy indicates to report an in-situ flow detection result of the target service flow. In this embodiment of this application, the controller may detect and analyze transmission performance of only some key service flows (including the target service flow), to reduce data processing pressure of the controller. Correspondingly, the controller may send a sending policy of the key service flow to the network device, to indicate the network device to report an in-situ flow detection result of the key service flow, and in-situ flow detection results of other non-key service flows do not need to be reported.

[0313] In this embodiment of this application, the third network device may be a node on a forwarding path (for example, a forwarding path in the first network service) of the target service flow, and the third network device may be an ingress node, a transit node, or an egress node on an in-situ flow detection path of the target service flow. In addition, the third network device and the first network device may be a same network device, or may be different network devices.

[0314] Optionally, the sending policy may include a value of one or more fields in the application-aware identifier of the target service flow. For example, the sending policy may include one or more of the following information: an application identifier of an application to which the target service flow belongs, a user identifier of a user to which the target service flow belongs, a flow identifier of the target service flow, and an SLA level of the target service flow.

[0315] For example, refer to FIG. 1. If the first network device is 02b, and the third network device includes network devices 02c and 02d, the controller 01 may separately deliver the sending policy of the target service flow to the network devices 02b, 02c, and 02d.

[0316] Step 605: If determining that the received target service flow is a service flow indicated by the first application-aware identifier, the first network device forwards a service packet of the target service flow by using the first network service and based on the correspondence.

[0317] For an implementation process of step 605, refer to the related descriptions of step 408.

[0318] Step 606: The third network device performs, based on in-situ flow detection information in the service packet, in-situ flow detection on the target service flow to which the service packet belongs, to obtain the in-situ flow detection result.

[0319] In this embodiment of this application, the third network device may receive the service packet that is of the target service flow and that is forwarded by the first network device. If the service packet includes the in-situ flow detection information (for example, IFIT information), the third network device may perform, based on the in-situ flow detection information, in-situ flow detection on the target service flow to which the service packet belongs, to obtain the in-situ flow detection result. The in-situ flow detection result may include a measurement result of a performance indicator such as a latency and/or a packet loss rate of the target service flow.

[0320] It may be understood that the in-situ flow detection information may be encapsulated in the service packet by the ingress node on the in-situ flow detection path of the target service flow. The ingress node may be a second network device, or may be the first network device, or may be a downstream network device of a first network device, for example, may be the third network device. If the ingress node is the third network device, the third network device may encapsulate the in-situ flow detection information in the service packet of the target service flow, and may perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain the in-situ flow detection result.

[0321] Step 607: The third network device sends the in-situ flow detection result and a target application-aware identifier to the controller based on the indication of the sending policy.

[0322] In this embodiment of this application, the third network device may obtain the target application-aware identifier of the target service flow. If determining, based on the target application-aware identifier and the sending policy, that the target service flow is a key service flow whose in-situ flow detection result needs to be reported, the third network device may send the in-situ flow detection result and the target application-aware identifier of the target service flow to the controller.

[0323] Optionally, the sending policy of the target service flow may include a value of one or more fields in the application-aware identifier of the target service flow. After obtaining the target application-aware identifier of the target service flow, the third network device may detect whether a value of each field in the sending policy matches a value of a corresponding field in the target application-aware identifier. If a value of each field in the sending policy matches a value of a corresponding field in the target application-aware identifier, the third network device may determine that the target service flow is the key service flow whose in-situ flow detection result needs to be reported, and report the in-situ flow detection result and the target application-aware identifier of the target service flow to the controller.

[0324] It may be understood that, after obtaining an application-aware identifier of a service flow, if detecting that a value of any field in the sending policy does not match a value of a corresponding field in the application-aware identifier, the third network device may determine that the service flow is not a key service flow, and does not need to report an in-situ flow detection result and an application-aware identifier of the service flow.

[0325] For example, refer to FIG. 1. It is assumed that the sending policy includes: a user identifier=UID 1. If a target application-aware identifier that is of a target service flow and that is obtained by the third network devices 02c and 02d includes a user identifier, and the user identifier is the UID 1, both the third network devices 02c and 02d may determine that the target service flow is a key service flow, and may report an in-situ flow detection result and the target application-aware identifier of the target service flow. If a user identifier in an application-aware identifier that is of a service flow and that is obtained by the third network device is a UID 2, the third network device may determine that the service flow is not a key service flow, and does not need to report an in-situ flow detection result and the application-aware identifier of the service flow.

[0326] The third network device may report, according to the sending policy delivered by the controller, only the in-situ flow detection result of the key service flow, and does not need to report the in-situ flow detection result of the non-key service flow. Therefore, a data amount of the in-situ flow detection result that needs to be received and processed by the controller is reduced, that is, data processing pressure of the controller is reduced, and a reporting granularity of the in-situ flow detection result is flexibly adjusted. In addition, because the data amount of the in-situ flow detection result that needs to be reported by the third network device is reduced, a transmission resource occupied by the in-situ flow detection result can be further effectively reduced.

[0327] In a possible implementation, the third network device may obtain the target application-aware identifier of the target service flow from the service packet of the target service flow. The target application-aware identifier may be the first application-aware identifier delivered by the controller, or may be a second application-aware identifier generated by the network device.

[0328] In this implementation, the target application-aware identifier may be encapsulated in the service packet by an application-aware edge device (namely, the foregoing second network device); or may be encapsulated in the service packet by the ingress node on the in-situ flow detection path of the target service flow; or may be encapsulated in the service packet by a headend network device (namely, the foregoing first network device) configured to forward the first network service of the target service flow; or may be encapsulated in the service packet by an application to which the target service flow belongs.

[0329] Optionally, if the in-situ flow detection information in the service packet is IFIT information, as shown in FIG. 12, the target application-aware identifier may be encapsulated in a flow identifier field of the IFIT information. That is, the target application-aware identifier may be replaced with FlowMonID in the IFIT information. Alternatively, the target application-aware identifier may be encapsulated in a reserved (reserved) field of the IFIT information. That is, the IFIT information may include the FlowMonID, and also include the target application-aware identifier.

[0330] In another possible implementation, the target application-aware identifier of the target service flow is not encapsulated in the service packet that is of the target service flow and that is received by the third network device. In this implementation, the controller may further deliver an identifier generation rule to the third network device. After receiving the service packet of the target service flow, the third network device may generate the second application-aware identifier of the target service flow according to the identifier generation rule delivered by the controller. Correspondingly, the foregoing target application-aware identifier may be the second application-aware identifier generated by the third network device. For a process in which the third network device generates the second application-aware identifier, refer to step 405.

[0331] Alternatively, the controller may further deliver the correspondence between the first application-aware identifier and the first network service to the third network device. After receiving the service packet of the target service flow, the third network device may determine, in a manner of parsing the packet or analyzing a traffic feature, that the target service flow is the service flow indicated by the first application-aware identifier. In other words, the third network device may determine, in the manner of parsing the packet or analyzing the traffic feature, that the application-aware identifier of the target service flow is the first application-aware identifier. Correspondingly, the foregoing target application-aware identifier may alternatively be the first application-aware identifier delivered by the controller.

[0332] It may be understood that, if the target application-aware identifier is not encapsulated in the service packet that is of the target service flow and that is received by the third network device, after the third network device obtains the target application-aware identifier of the target service flow, the third network device may encapsulate the target application-aware identifier in the service packet of the target service flow, and forward the service packet in which the target application-aware identifier is encapsulated.

[0333] For example, assuming that the service packet that is of the target service flow and that is received by the third network device includes the IFIT information, the third network device may encapsulate the target application-aware identifier in the flow identifier field or the reserved field of the IFIT information. Certainly, the third network device may alternatively encapsulate the target application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0334] It may be further understood that, if the target application-aware identifier in the service packet received by the third network device is encapsulated in the destination address field, the HBH, the DOH, or the SRH, the third network device may alternatively extract the target application-aware identifier from an original encapsulation location, and re-encapsulate the target application-aware identifier in the flow identifier field or the reserved field of the IFIT information. Then, the third network device may forward the re-encapsulated service packet.

[0335] Step 608: The controller analyzes transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

[0336] In this embodiment of this application, after receiving the in-situ flow detection result and the target application-aware identifier that are sent by the third network device, the controller can analyze the transmission performance of the target service flow by using a granularity indicated by at least one identifier in the target application-aware identifier. The transmission performance may be represented by using a performance indicator such as a packet loss rate and/or a latency.

[0337] In an in-situ flow detection scenario, the controller may receive an in-situ flow detection result reported by at least one third network device on the in-situ flow detection path of the target service flow, and the controller may analyze the transmission performance of the target service flow based on the received at least one in-situ flow detection result. The at least one third network device may include an ingress node, an intermediate node, and/or an egress node on the in-situ flow detection path.

[0338] For example, if the at least one third network device includes the ingress node and the egress node, the controller may implement end-to-end detection on the transmission performance of the target service flow. If the at least one third network device includes the ingress node, the intermediate node, and the egress node, the controller may implement hop-by-hop detection on the transmission performance of the target service flow.

[0339] It may be understood that the controller may receive in-situ flow detection results and application-aware identifiers that are of different service flows and that are reported by different network devices, and the controller may determine an in-situ flow detection result of a same service flow based on the application-aware identifier, and may further analyze transmission performance of the service flow based on one or more in-situ flow detection results of the same service flow.

[0340] It may be further understood that the target service flow indicated by the target application-aware identifier may be a specified data flow, or may be a group of data flows. In other words, the target service flow may include a plurality of data flows. For example, the group of data flows may include data flows of different applications used by a same user, or data flows of different users under a same application. If the target service flow is a group of data flows, the controller may analyze transmission performance of data flows in this group of service flows based on a received in-situ flow detection result, or may analyze overall transmission performance of this group of service flows, which may also be referred to as average transmission performance.

[0341] Optionally, in step 607, when sending the in-situ flow detection result and the target application-aware identifier to the controller, the third network device may further report a corresponding in-situ flow detection flow identifier. The in-situ flow detection flow identifier may be obtained from the in-situ flow detection information. For example, the in-situ flow detection flow identifier may be a monitoring flow identifier (FlowMonID) in the IFIT information. The in-situ flow detection flow identifier may indicate a monitored data flow in the target service flow, which may be understood as that the in-situ flow detection result is a detection result for the data flow indicated by the in-situ flow detection flow identifier.

[0342] Correspondingly, the controller may determine, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and may further analyze, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0343] In a scenario in which the target service flow includes a plurality of monitored data flows, because each monitored data flow has a unique in-situ flow detection flow identifier (for example, FlowMonID), the controller may further generate a correspondence between the target application-aware identifier and a plurality of in-situ flow detection flow identifiers. When analyzing the transmission performance of the target service flow, the controller may analyze transmission performance of each monitored data flow included in the target service flow. Then, the controller may further determine the overall transmission performance (for example, the average transmission performance) of the target service flow based on the transmission performance of each monitored data flow. For example, the controller may calculate a packet loss rate of each monitored data flow in the target service flow, and use an average value of the packet loss rates of the monitored data flows as an average packet loss rate of the target service flow.

[0344] Step 609: The controller displays the performance indicator of the target service flow based on a target granularity.

[0345] The performance indicator indicates the transmission performance of the target service flow. For example, the performance indicator may include at least one of a packet loss rate and a latency. The target granularity is a granularity indicated by the at least one identifier in the target application-aware identifier. Because the target application-aware identifier may include at least one of a user identifier and an application identifier, the controller can display the performance indicator of the service flow by using a user and/or an application as a granularity. If the target application-aware identifier further includes a flow identifier (namely, a session ID) and an SLA level, the controller can further display the performance indicator of the service flow by using the flow identifier and/or the SLA level as a granularity.

[0346] It may be understood that the target granularity may be flexibly configured and adjusted based on a requirement of an application scenario, for example, may be configured and adjusted by operations and maintenance personnel.

[0347] If the target granularity is a user granularity, the controller can display a performance indicator of at least one service flow of each user in one or more users by using a user as a unit. For each user, the controller may display a performance indicator of each service flow (for example, a service flow of each application used by the user) of the user, or may display an average value of the performance indicators of a plurality of service flows of the user.

[0348] If the target granularity is an application granularity, the controller can display a performance indicator of at least one service flow of each of one or more applications by using an application as a unit. For each application, the controller may display a performance indicator of each service flow (for example, a service flow of each user who uses the application) of the application, or may display an average value of performance indicators of a plurality of service flows of the application. The average value may be an arithmetic average value, a root mean square average value, or a weighted average value.

[0349] If the target granularity is a user+application granularity, the controller can display, by using a user and an application as a unit, a performance indicator of at least one service flow that has a same user identifier and a same application identifier.

[0350] For example, it is assumed that the controller obtains in-situ flow detection results of a total of three service flows: a service flow 1 to a service flow 3, and application-aware identifiers of the three service flows are shown in Table 2. If the target granularity is the user granularity, and a user identifier of a target user whose performance indicator needs to be displayed is a UID 1, the controller may separately display performance indicators of the service flow 1 and the service flow 2, or the controller may calculate and display an average value of performance indicators of the service flow 1 and the service flow 2.

[0351] If the target granularity is the application granularity, and an application identifier of a target application whose performance indicator needs to be displayed is an AID 1, the controller may separately display performance indicators of the service flow 1 and the service flow 3, or the controller may calculate and display an average value of performance indicators of the service flow 1 and the service flow 3.

[0352] If the target granularity is the user+application granularity, a user identifier of the service flow whose performance indicator needs to be displayed is a UID 1, and an application identifier is an AID 2, the controller may display the performance indicator of the service flow 2.

Table 2

Service flow	Application-aware identifier	
	User identifier	Application identifier
Service flow 1	UID 1	AID 1
Service flow 2	UID 1	AID 2
Service flow 3	UID 2	AID 1

[0353] It can be learned based on the foregoing analysis that the application-aware identifier of the service flow may include information in a plurality of different dimensions of the service flow. Therefore, the performance indicator of the service flow is displayed by using the granularity indicated by the identifier in the application-aware identifier, so that refined visualization of the performance indicator can be implemented. In addition, a display granularity of the performance indicator may be further flexibly adjusted based on a requirement, so that flexibility of displaying the performance indicator is effectively improved.

[0354] Step 610: If determining, based on the transmission performance, that the first network service does not meet the user requirement of the target service flow, the controller determines that a network service required for transmitting the target service flow is a second network service.

[0355] In this embodiment of this application, because the target application-aware identifier that is of the target service flow and that is reported by the third network device matches the first application-aware identifier generated by the controller, the controller may determine that the target service flow is the service flow indicated by the first application-aware identifier. Further, the controller may determine the user requirement of the target service flow, and may detect, based on the transmission performance that is of the target service flow and that is obtained through analysis, whether the transmission performance meets the user requirement of the target service flow. If determining that the transmission performance of the target service flow does not meet the user requirement of the target service flow, the controller may further recalculate the second network service that can meet the user requirement of the target service flow, that is, the controller may update the network service of the target service flow from the first network service to the second network service.

[0356] It may be understood that if the controller determines that the transmission performance of the target service flow can meet the user requirement of the target service flow, the network service used to transmit the target service flow does not need to be updated.

[0357] Step 611: The controller sends a correspondence between the first application-aware identifier and the second network service to the first network device.

[0358] The controller may re-deliver the correspondence between the first application-aware identifier and the second network service to the first network device, for example, may deliver a correspondence between the first application-aware identifier and an identifier of the second network service. After receiving the correspondence, the first network device may forward the service packet of the target service flow by using the second network service.

[0359] In a process of transmitting the target service flow, the controller may analyze the transmission performance of the target service flow based on the in-situ flow detection result, and adjust, in time based on the transmission performance, the network service allocated to the target service flow. Therefore, closed-loop dynamic optimization of a network resource is implemented, and the transmission performance of the target service flow is effectively ensured.

[0360] For example, it is assumed that the first application-aware identifier of the target service flow is an APN ID 1, an identifier of the first network service is a BSID 1, and the second network service recalculated by the controller is an SRv6 path indicated by a BSID 2. Refer to FIG. 1. The controller 01 may deliver a correspondence between the APN ID 1 and the BSID 2 to the network device 02b. The network device 02b may subsequently forward the service packet of the target service flow through the SRv6 path indicated by the BSID 2.

[0361] It may be understood that, in a scenario in which the first network device and the application-aware edge device (namely, the foregoing second network device) are different devices, the controller may further send the correspondence between the first application-aware identifier and the second network service to the second network device. For example, refer to FIG. 1. The controller 01 may further send the correspondence between the first application-aware identifier and the second network service to the network device 02a.

[0362] Optionally, in step 607, the third network device may alternatively not need to detect, according to the sending policy, whether the target service flow is the key service flow, but may directly report the in-situ flow detection result and the target application-aware identifier of the target service flow to the controller. In other words, if detecting that the service packet includes in-situ flow detection information, the third network device may perform, based on the in-situ flow detection information, in-situ flow detection on the service flow to which the service packet belongs, and directly report the in-situ flow detection result and the application-aware identifier of the service flow to the controller.

[0363] In a possible example, step 604 may be deleted based on a situation. To be specific, the controller does not need to deliver the sending policy of the target service flow. Correspondingly, the third network device does not need to detect, according to the sending policy, whether the target service flow is the key service flow.

[0364] In another possible example, the third network device may have an application-aware identifier processing function. If the application-aware identifier processing function is enabled, the third network device may detect, based on the target application-aware identifier and the sending policy, whether the target service flow is the key service flow. If the application-aware identifier processing function is disabled, the third network device does not need to detect, according to the sending policy, whether the target service flow is the key service flow.

[0365] Optionally, the third network device may enable or disable the application-aware identifier processing function of the third network device based on a received configuration instruction. The configuration instruction may be delivered by the controller, or may be directly configured by the operations and maintenance personnel.

[0366] It may be further understood that, after receiving the service packet of the target service flow, the third network device may further first detect, according to the sending policy, whether the target service flow is the key service flow. If determining that the target service flow is the key service flow, the third network device may perform step 606 to obtain the in-situ flow detection result of the target service flow. If determining that the target service flow is not the key service flow, the third network device does not need to perform step 606, to be specific, the third network device does not need to perform in-situ flow detection on the non-key service flow.

[0367] It may be further understood that, in a possible implementation, in step 601, the controller may send the sending policy of the target service flow to each node on the in-situ flow detection path of the target service flow. In this case, each node on the in-situ flow detection path may detect, based on the method shown in step 607, whether the received service flow is the key service flow.

[0368] In another possible implementation, the controller may send the sending policy of the target service flow to only the application-aware edge device (namely, the second network device). The second network device may determine, based on the target application-aware identifier of the target service flow and the sending policy, that the target service flow is the key service flow whose in-situ flow detection result needs to be reported, and may add mark information to the service packet of the target service flow. A downstream network device (for example, the third network device) of the second network device may further determine, based on the mark information, that the target service flow is the key service flow. Correspondingly, in this implementation, the third network device may directly determine, based on the mark information in the service packet, whether the service flow to which the service packet belongs is the key service flow.

[0369] It may be further understood that an execution sequence of the steps in the foregoing packet forwarding method may be adjusted based on a situation, or the steps may be added or deleted based on a situation. For example, step 604 may be performed before step 603; or step 609 may be deleted based on a situation; or step 610 and step 611 may be performed before step 609; or step 610 and step 611 may be deleted based on a situation.

[0370] In conclusion, this embodiment of this application provides a packet forwarding method. When reporting an in-situ flow detection result of a target service flow to the controller, the network device may also report a target application-aware identifier of the target service flow. Further, the controller can detect and analyze transmission performance of the service flow by using a granularity indicated by at least one identifier in the target application-aware identifier, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved. In addition, the controller may further display a performance indicator of the service flow based on the granularity indicated by the at least one identifier in the target application-aware identifier. Therefore, refined and flexible visualization of the performance indicator is implemented.

[0371] FIG. 13 is a schematic diagram of a structure of a controller according to an embodiment of this application. The controller may be used in the communication network shown in FIG. 1 or FIG. 7, and may implement steps performed by the controller in the embodiment shown in FIG. 2, FIG. 6, FIG. 10, or FIG. 11. Refer to FIG. 13. The controller includes: a generation module 011, configured to obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow. For implementation of a function of the generation module 011, refer to the related descriptions of step 101, step 402, or step 602 in the foregoing method embodiment.

[0372] A sending module 012 is configured to send the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow. For implementation of a function of the sending module 012, refer to the related descriptions of step 102, step 403, step 505, or step 603 in the foregoing method embodiment.

[0373] Optionally, the correspondence includes an identifier of the first network service, and the identifier of the first network service includes: a binding segment identifier and/or an identifier of a network slice.

[0374] Optionally, the first application-aware identifier includes at least one of a user identifier and an application identifier.

[0375] Optionally, the first application-aware identifier further includes at least one of a flow identifier, an SLA level, or a service requirement.

[0376] Optionally, the sending module 012 is further configured to send an identifier generation rule to the first network device, so that the first network device generates a second application-aware identifier of the target service flow according to the identifier generation rule, and the second application-aware identifier is used to match the first application-aware identifier to determine the first network service. For implementation of a function of the sending module 012, further refer to the related descriptions of step 404 in the foregoing method embodiment.

[0377] Optionally, the sending module 012 is further configured to send the first application-aware identifier of the target service flow to a second network device, where the first application-aware identifier is used by the second network device to encapsulate the application-aware identifier of the target service flow in the service packet of the target service flow if the second network device determines that the received service flow is the target service flow. For implementation of a function of the sending module 012, further refer to the related descriptions of step 503 in the foregoing method embodiment.

[0378] Optionally, as shown in FIG. 14, the controller may further include: an obtaining module 013, configured to obtain the user requirement of the target service flow through a northbound interface. For implementation of a function of the obtaining module 013, refer to the related descriptions of step 401, step 501, or step 601 in the foregoing method embodiment.

[0379] Optionally, still refer to FIG. 14. The controller may further include:

a receiving module 014, configured to receive an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the target application-aware identifier is an application-aware identifier of a service flow to which the in-situ flow detection result belongs, and the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is generated by the network device. For implementation of a function of the receiving module 014, refer to the related descriptions of step 607 in the foregoing method embodiment.

[0380] An analysis module 015 is configured to analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier. For implementation of a function of the analysis module 015, refer to the related descriptions of step 608 in the foregoing method embodiment.

[0381] Optionally, as shown in FIG. 14, the controller may further include:

a display module 016, configured to display a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

[0382] For implementation of a function of the display module 016, refer to the related descriptions of step 609 in the foregoing method embodiment.

[0383] Optionally, the generation module 011 is further configured to: determine, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; and determine that a network service required for transmitting the target service flow is a second network service. For implementation of a function of the generation module 011, refer to the related descriptions of step 610 in the foregoing method embodiment.

[0384] The sending module 012 is further configured to send a correspondence between the first application-aware identifier and the second network service to the first network device. For implementation of a function of the sending module 012, further refer to the related descriptions of step 611 in the foregoing method embodiment.

[0385] Optionally, the sending module 012 is further configured to send a sending policy of the target service flow to the first network device and/or the third network device before the receiving module 014 receives the in-situ flow detection result and the target application-aware identifier that are sent by the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow. For implementation of a function of the sending module 012, further refer to the related descriptions of step 604 in the foregoing method embodiment.

[0386] Optionally, the receiving module 014 may be configured to receive the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device. The in-situ flow detection flow identifier is also referred to as a monitoring flow identifier, and may indicate a monitored data flow in the target service flow.

[0387] The analysis module 015 may be configured to: determine, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyze, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0388] Optionally, the user requirement of the target service flow includes one or more of the following requirements:

a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

[0389] In conclusion, this embodiment of this application provides a controller, where the controller may obtain a correspondence between an application-aware identifier of a service flow and a network service required for transmitting the service flow, and deliver the correspondence to a network device. Further, when identifying the service flow as a service flow indicated by the application-aware identifier, the network device may directly forward a packet of the service flow by using the corresponding network service. The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

[0390] FIG. 15 is a schematic diagram of a structure of a network device according to an embodiment of this application. The network device may be used in the communication network shown in FIG. 1 or FIG. 7. For example, the network device may be the network device 02a, 02c, or 02d in FIG. 1 or FIG. 7, or may be the network device 02b shown in FIG. 1. In addition, the network device may implement steps performed by at least one of the first network device, the second network device, and the third network device in the embodiment shown in FIG. 2, FIG. 6, FIG. 10, or FIG. 11. Refer to FIG. 15. The network device includes:

a receiving module 021, configured to receive a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller in the network, where the first application-aware identifier is generated by the controller based on a user requirement of a service flow. For implementation of a function of the receiving module 021, refer to the related descriptions of step 102, step 403, step 505, or step 603 in the foregoing method embodiment.

[0391] A sending module 022 is configured to: if the received target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence. For implementation of a function of the sending module 022, refer to the related descriptions of step 103, step 408, step 508, or step 605 in the foregoing method embodiment.

[0392] Optionally, as shown in FIG. 16, the network device may further include:

an obtaining module 023, configured to obtain a second application-aware identifier of the target service flow from the service packet of the target service flow; and

a determining module 024, configured to: if the second application-aware identifier matches the first application-aware identifier, determine that the target service flow is the service flow indicated by the first application-aware identifier.

[0393] Optionally, the service packet received by the network device includes IFIT information, and the second application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information. Alternatively, the second application-aware identifier is encapsulated in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0394] Optionally, the second application-aware identifier is encapsulated in a BSID field of the SRH field.

[0395] Optionally, the receiving module 021 may be further configured to receive an identifier generation rule sent by the controller. For implementation of a function of the receiving module 021, further refer to the related descriptions of step 404 in the foregoing method embodiment.

[0396] Still refer to FIG. 16. The network device may further include:

a generation module 025, configured to generate a second application-aware identifier of the target service flow according to the identifier generation rule. For implementation of a function of the generation module 025, refer to the related descriptions of step 405 in the foregoing method embodiment.

[0397] The determining module 024 is configured to: if the second application-aware identifier matches the first application-aware identifier, determine that the target service flow is the service flow indicated by the first application-aware identifier. For implementation of a function of the determining module 024, refer to the related descriptions of step 406 in the foregoing method embodiment.

[0398] Optionally, the service packet received by the network device includes IFIT information. The sending module 022 may be configured to: encapsulate the target application-aware identifier in a flow identifier field or a reserved field of the IFIT information, and forward, by using the first network service, the service packet in which the target application-aware identifier is encapsulated. For implementation of a function of the sending module 022, further refer to the related descriptions of step 406 or step 506 in the foregoing method embodiment.

[0399] Optionally, as shown in FIG. 16, the network device may further include:

a detection module 026, configured to: if the service packet that is of the target service flow and that is received by the receiving module 021 includes in-situ flow detection information, perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result. For implementation of a function of the detection module 026, refer to the related descriptions of step 606 in the foregoing method embodiment.

[0400] The sending module 022 is further configured to send the in-situ flow detection result and the target application-aware identifier to the controller, where the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is obtained by the network device. For implementation of a function of the sending module 022, further refer to the related descriptions of step 607 in the foregoing method embodiment.

[0401] Optionally, the receiving module 021 may be further configured to receive a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow. For implementation of a function of the receiving module 021, further refer to the related descriptions of step 604 in the foregoing method embodiment.

[0402] The sending module 022 may be configured to send the in-situ flow detection result and the target application-aware identifier to the controller based on the indication of the sending policy.

[0403] Optionally, the sending module 022 may be configured to send the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller. The in-situ flow detection flow identifier may indicate a monitored data flow in the target service flow.

[0404] In conclusion, this embodiment of this application provides a network device. The network device may receive a correspondence that is between an application-aware identifier of a service flow and a network service required for transmitting the service flow and that is delivered by a controller, and when identifying the service flow as a service flow indicated by the application-aware identifier, may directly forward a packet of the service flow by using the corresponding network service. The controller may establish and deliver the correspondence between the application-aware identifier of the service flow and the network service, so that the network device can directly forward the service packet of the service flow based on the correspondence. Therefore, flexibility of forwarding the service packet is effectively improved.

[0405] FIG. 17 is a schematic diagram of a structure of a packet forwarding apparatus according to an embodiment of this application. The packet forwarding apparatus may be used in the communication network shown in FIG. 1 or FIG. 7, and may implement the steps in the embodiment shown in FIG. 4. Refer to FIG. 17. The packet forwarding apparatus includes:

a generation module 001, configured to generate a first application-aware identifier of a target service flow based on a user requirement of the target service flow, where the first application-aware identifier is used by a network device to encapsulate a target application-aware identifier in a service packet of the target service flow, the target application-aware identifier is the first application-aware identifier or a second application-aware identifier matching the first application-aware identifier, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the target service flow. For implementation of a function of the generation module 001, refer to the related descriptions of step 201 in the foregoing method embodiment.

[0406] A sending module 002 is configured to send the first application-aware identifier, where the first application-aware identifier is used by the network device to forward the service packet of the target service flow by using the first network service. For implementation of a function of the sending module 002, refer to the related descriptions of step 202 in the foregoing method embodiment.

[0407] In a possible implementation, the packet forwarding apparatus may be used in a controller in the communication network shown in FIG. 1 or FIG. 7, and may further implement steps performed by the controller in the embodiment shown in FIG. 6, FIG. 10, or FIG. 11.

[0408] The generation module 001 may be configured to generate the first application-aware identifier of the target service flow based on the obtained user requirement of the target service flow. For implementation of a function of the generation module 001, further refer to the related descriptions of step 402, step 502, or step 602 in the foregoing method embodiment.

[0409] The sending module 002 is configured to send the first application-aware identifier to a second network device, so that the second network device encapsulates the target application-aware identifier in the service packet of the target service flow. For implementation of a function of the sending module 002, further refer to the related descriptions of step 503 in the foregoing method embodiment.

[0410] Optionally, as shown in FIG. 18, the apparatus may further include:

an obtaining module 003, configured to obtain the user requirement of the target service flow through a northbound interface. For implementation of a function of the obtaining module 003, refer to the related descriptions of step 401, step 501, or step 601 in the foregoing method embodiment.

[0411] Optionally, the generation module 001 is further configured to determine, based on the user requirement of the target service flow, the first network service required for transmitting the target service flow. For implementation of a function of the generation module 001, further refer to the related descriptions of step 503 in the foregoing method embodiment.

[0412] The sending module 002 is further configured to send a correspondence between the first application-aware identifier and the first network service to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward the service packet of the target service flow. For implementation of a function of the sending module 002, further refer to the related descriptions of step 403, step 505, or step 603 in the foregoing method embodiment.

[0413] Optionally, still refer to FIG. 18. The apparatus may further include:
a receiving module 004, configured to receive an in-situ flow detection result and the target application-aware identifier that are sent by a third network device. For implementation of a function of the receiving module 004, refer to the related descriptions of step 607 in the foregoing method embodiment.

[0414] An analysis module 005 is configured to analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier. For implementation of a function of the analysis module 005, refer to the related descriptions of step 608 in the foregoing method embodiment.

[0415] Optionally, as shown in FIG. 18, the apparatus may further include:
a display module 006, configured to display a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier. For implementation of a function of the display module 006, refer to the related descriptions of step 609 in the foregoing method embodiment.

[0416] Optionally, the receiving module 004 may be configured to receive the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device.

[0417] The analysis module 005 may be configured to: determine, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyze, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0418] Optionally, the generation module 001 may be further configured to: determine, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow; and determine that a network service required for transmitting the target service flow is a second network service. For implementation of a function of the generation module 001, further refer to the related descriptions of step 610 in the foregoing method embodiment.

[0419] The sending module 002 may be further configured to send a correspondence between the first application-aware identifier and the second network service to the first network device. For implementation of a function of the sending module 002, further refer to the related descriptions of step 611 in the foregoing method embodiment.

[0420] Optionally, the sending module 002 may be further configured to send a sending policy of the target service flow to the second network device and/or the third network device before the receiving module 004 receives the in-situ flow detection result and the target application-aware identifier that are sent by the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow. For implementation of a function of the sending module 002, further refer to the related descriptions of step 604 in the foregoing method embodiment.

[0421] In another possible implementation, the packet forwarding apparatus may be used in a network device in the communication network shown in FIG. 1 or FIG. 7, and may further implement steps performed by at least one of the first network device, the second network device, and the third network device in the embodiment shown in FIG. 6, FIG. 10, or FIG. 11.

[0422] The generation module 001 may be configured to generate a first application-aware identifier of a target service flow based on a user requirement that is of the target service flow and that is sent by a controller. For implementation of a function of the generation module 001, further refer to the related descriptions of step 502.

[0423] The sending module 002 may be configured to: encapsulate the first application-aware identifier in a service packet of the target service flow, and forward the service packet in which the first application-aware identifier is encapsulated. For implementation of a function of the sending module 002, further refer to the related descriptions of step 506 and step 507 in the foregoing method embodiment.

[0424] Optionally, if the service packet that is of the target service flow and that is received by the second network device includes in-situ flow detection information, as shown in FIG. 19, the apparatus may further include:
a detection module 007, configured to perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result. For implementation of a function of the detection module 007, refer to the related descriptions of step 606 in the foregoing method embodiment.

[0425] The sending module 002 may be further configured to send the in-situ flow detection result and the first application-aware identifier to the controller. For implementation of a function of the sending module 002, further refer to the related descriptions of step 607 in the foregoing method embodiment.

[0426] Optionally, still refer to FIG. 19. The apparatus may further include:
a receiving module 008, configured to receive a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow. For

implementation of a function of the receiving module 008, further refer to the related descriptions of step 604 in the foregoing method embodiment.

[0427] The sending module 002 may be configured to send the in-situ flow detection result and the first application-aware identifier to the controller based on the indication of the sending policy.

[0428] Optionally, the sending module 002 may be configured to send the in-situ flow detection result, the first application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

[0429] Optionally, the sending module 002 may be configured to: encapsulate the first application-aware identifier in a flow identifier field or a reserved field of IFIT information of the service packet; or encapsulate the first application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0430] Optionally, the user requirement of the target service flow includes one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

[0431] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier.

[0432] In conclusion, this embodiment of this application provides a packet forwarding apparatus. The packet forwarding apparatus can generate a first application-aware identifier based on a user requirement of a target service flow. The first application-aware identifier corresponds to a first network service, and is encapsulated in a service packet of the target service flow. Therefore, it can be ensured that a network device that receives the service packet can forward the service packet by using the corresponding first network service, so that flexibility of forwarding the service packet is effectively improved.

[0433] FIG. 20 is a schematic diagram of a structure of a network device according to an embodiment of this application. The network device may be used in the communication network shown in FIG. 1 or FIG. 7. For example, the network device may be the network device 02a, 02c, or 02d in FIG. 1 or FIG. 7, or may be the network device 02b shown in FIG. 1. In addition, the network device may implement steps in the embodiment shown in FIG. 4, or implement steps performed by at least one of the first network device, the second network device, and the third network device in the embodiment shown in FIG. 6, FIG. 10, or FIG. 11. Refer to FIG. 20. The network device includes:

a receiving module 021, configured to receive a first application-aware identifier sent by a controller, where the first application-aware identifier is generated based on a user requirement of a service flow, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the service flow. For implementation of a function of the receiving module 021, refer to the related descriptions of step 503 in the foregoing method embodiment.

[0434] An encapsulation module 027 is configured to: if the received target service flow is a service flow indicated by the first application-aware identifier, encapsulate a target application-aware identifier in a service packet of the target service flow, where the target application-aware identifier is the first application-aware identifier or a second application-aware identifier matching the first application-aware identifier. For implementation of a function of the encapsulation module 027, refer to the related descriptions of step 506 in the foregoing method embodiment.

[0435] A sending module 022 is configured to forward the service packet in which the target application-aware identifier is encapsulated. For implementation of a function of the sending module 022, refer to the related descriptions of step 507 in the foregoing method embodiment.

[0436] Optionally, if the service packet that is of the target service flow and that is received by the network device includes in-situ flow detection information, as shown in FIG. 20, the network device may further include:

a detection module 026, configured to perform in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result. For implementation of a function of the detection module 026, refer to the related descriptions of step 606 in the foregoing method embodiment.

[0437] The sending module 022 is further configured to send the in-situ flow detection result and the target application-aware identifier to the controller. For implementation of a function of the sending module 022, refer to the related descriptions of step 607 in the foregoing method embodiment.

[0438] Optionally, the sending module 022 may be configured to send the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

[0439] Optionally, the encapsulation module 027 may be configured to: encapsulate the target application-aware identifier in a flow identifier field or a reserved field of IFIT information of the service packet; or encapsulate the target application-aware identifier in a destination address field, an HBH, a DOH, or an SRH of the service packet.

[0440] Optionally, the receiving module 021 may be configured to receive a correspondence that is between the first application-aware identifier and the first network service and that is sent by the controller. For implementation of a function of the receiving module 021, further refer to the related descriptions of step 403, step 505, or step 603 in the foregoing method embodiment.

[0441] Correspondingly, the sending module 022 may be configured to forward, by using the first network service, the service packet in which the target application-aware identifier is encapsulated. For implementation of a function of the sending module 022, refer to the related descriptions of step 408, step 508, or step 605 in the foregoing method embodiment.

[0442] In conclusion, this embodiment of this application provides a network device. The network device may receive a first application-aware identifier that is of a target service flow and that is delivered by a controller, and encapsulate the first application-aware identifier in a service packet of the target service flow. The first application-aware identifier corresponds to a first network service. Therefore, it can be ensured that the network device that receives the service packet can forward the service packet by using the corresponding first network service, so that flexibility of forwarding the service packet is effectively improved.

[0443] FIG. 21 is a schematic diagram of a structure of a network device according to an embodiment of this application. The network device may be used in the communication network shown in FIG. 1 or FIG. 7. For example, the network device may be the network device 02a, 02c, or 02d in FIG. 1 or FIG. 7, or may be the network device 02b shown in FIG. 1. In addition, the network device may implement steps performed by at least one of the first network device, the second network device, and the third network device in the embodiment shown in FIG. 5, FIG. 6, FIG. 10, or FIG. 11. Refer to FIG. 21. The network device includes:

a detection module 026, configured to perform, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result. For implementation of a function of the detection module 026, refer to the related descriptions of step 301 and step 606 in the foregoing method embodiment.

[0444] A sending module 022 is configured to send the in-situ flow detection result and a target application-aware identifier of the target service flow to a controller in the network, where the target application-aware identifier is generated based on a user requirement of the target service flow, and the in-situ flow detection result and the target application-aware identifier are used by the controller to analyze transmission performance of the target service flow. For implementation of a function of the sending module 022, refer to the related descriptions of step 303 and step 607 in the foregoing method embodiment.

[0445] Optionally, the target application-aware identifier is encapsulated in the service packet, and the target application-aware identifier indicates a user and/or an application to which the target service flow belongs.

[0446] Optionally, if the in-situ flow detection information is IFIT information, the target application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information.

[0447] Optionally, as shown in FIG. 22, the network device may further include:

a receiving module 021, configured to receive a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller, where the first application-aware identifier is generated by the controller based on a user requirement of a service flow. For implementation of a function of the receiving module 021, refer to the related descriptions of step 403, step 505, or step 603 in the foregoing method embodiment.

[0448] The sending module 022 is further configured to: if the target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence. For implementation of a function of the sending module 022, refer to the related descriptions of step 408, step 508, or step 605 in the foregoing method embodiment.

[0449] Optionally, the receiving module 021 may be further configured to receive an identifier generation rule sent by the controller. For implementation of a function of the receiving module 021, further refer to the related descriptions of step 404 in the foregoing method embodiment.

[0450] A generation module 025 is configured to generate a second application-aware identifier of the target service flow according to the identifier generation rule. The target application-aware identifier is the second application-aware identifier or the first application-aware identifier that is of the target service flow and that is sent by the controller. For implementation of a function of the generation module 025, refer to the related descriptions of step 405 in the foregoing method embodiment.

[0451] Optionally, the in-situ flow detection information is IFIT information. As shown in FIG. 22, the network device may further include:

an encapsulation module 027, configured to encapsulate the target application-aware identifier in a flow identifier field or a reserved field of the IFIT information. For implementation of a function of the encapsulation module 027, refer to the related descriptions of step 506 in the foregoing method embodiment.

[0452] The sending module 022 may be further configured to forward the service packet in which the target application-aware identifier is encapsulated. For implementation of a function of the sending module 022, further refer to the related descriptions of step 507 in the foregoing method embodiment.

[0453] Optionally, the receiving module 021 may be further configured to receive a sending policy that is of the target service flow and that is sent by the controller, where the sending policy indicates to report the in-situ flow detection result of the target service flow. For implementation of a function of the receiving module 021, further refer to the related descriptions of step 604 in the foregoing method embodiment.

[0454] The sending module 022 is configured to send the in-situ flow detection result and the target application-aware identifier of the target service flow to the controller based on the indication of the sending policy.

[0455] Optionally, the sending module 022 may be configured to send the in-situ flow detection result, the target application-aware identifier of the target service flow, and a corresponding in-situ flow detection flow identifier to the controller in the network.

[0456] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier.

[0457] In conclusion, this embodiment of this application provides a network device. When reporting an in-situ flow detection result of a target service flow to a controller, the network device may also report a target application-aware identifier of the target service flow. Further, the controller can detect and analyze transmission performance of the service flow by using a granularity indicated by at least one identifier in the target application-aware identifier, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved.

[0458] FIG. 23 is a schematic diagram of a structure of still another controller according to an embodiment of this application. The controller may be used in the communication network shown in FIG. 1 or FIG. 7, and may implement steps performed by the controller in the embodiment shown in FIG. 5, FIG. 6, FIG. 10, or FIG. 11. Refer to FIG. 23. The controller includes:

a receiving module 014, configured to receive an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the in-situ flow detection result is obtained by the third network device by performing in-situ flow detection on a target service flow, and the target application-aware identifier is generated based on a user requirement of the target service flow. For implementation of a function of the receiving module 014, refer to the related descriptions of step 607 in the foregoing method embodiment.

[0459] An analysis module 015 is configured to analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier. For implementation of a function of the analysis module 015, refer to the related descriptions of step 608 in the foregoing method embodiment.

[0460] Optionally, the target application-aware identifier includes at least one of a user identifier and an application identifier. As shown in FIG. 14, the controller may further include:

a display module 016, configured to display a performance indicator of the target service flow based on a target granularity, where the performance indicator indicates the transmission performance of the target service flow; and the target granularity is a granularity indicated by the at least one identifier in the target application-aware identifier. For implementation of a function of the display module 016, refer to the related descriptions of step 609 in the foregoing method embodiment.

[0461] Optionally, still refer to FIG. 14. The controller may further include:

a sending module 012, configured to send a sending policy of the target service flow to the third network device before the receiving module 014 receives the in-situ flow detection result and the target application-aware identifier that are sent by the third network device, where the sending policy indicates to report the in-situ flow detection result of the target service flow. For implementation of a function of the sending module 012, further refer to the related descriptions of step 604 in the foregoing method embodiment.

[0462] Optionally, the receiving module 011 may be configured to receive the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device. Correspondingly, the analysis module 012 may be configured to: determine, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow included in the target service flow; and analyze, based on the in-situ flow detection result, transmission performance of the at least one data flow included in the target service flow.

[0463] Optionally, as shown in FIG. 14, the controller may further include:

a generation module 011, configured to obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow. For implementation of a function of the generation module 011, refer to the related descriptions of step 402 or step 602 in the foregoing method embodiment.

[0464] The sending module 012 is further configured to send the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow. The target application-aware identifier is the first application-aware identifier or a second application-aware identifier that is of the target service flow and that is generated by the network device. For implementation of a function of the sending module 012, refer to the related descriptions of step 403, step 505, or step 603 in the foregoing method embodiment.

[0465] Optionally, the generation module 011 is further configured to: if determining, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow, determine that a network service required for transmitting the target service flow is a second network service. For implementation of a function of the generation module 011, refer to the related descriptions of step 610 in the foregoing method embodiment.

[0466] The sending module 012 is further configured to send a correspondence between the first application-aware identifier and the second network service to the first network device. For implementation of a function of the sending module 012, further refer to the related descriptions of step 611 in the foregoing method embodiment.

[0467] Optionally, the sending module 012 is further configured to send the first application-aware identifier of the target service flow to a second network device. For implementation of a function of the sending module 012, further refer to the related descriptions of step 503 in the foregoing method embodiment.

[0468] Optionally, refer to FIG. 14. The controller may further include:

an obtaining module 013, configured to obtain the user requirement of the target service flow through a northbound interface. For implementation of a function of the obtaining module 013, refer to the related descriptions of step 401, step 501, or step 601 in the foregoing method embodiment.

[0469] In conclusion, this embodiment of this application provides a controller. When receiving an in-situ flow detection result that is of a target service flow and that is reported by a network device, the controller may receive a target application-aware identifier that is of the target service flow and that is also reported by the network device. Therefore, the controller can detect and analyze transmission performance of the service flow by using a granularity indicated by at least one identifier in the target application-aware identifier, so that flexibility of detecting and analyzing the transmission performance of the service flow is effectively improved.

[0470] It may be clearly understood by a person skilled in the art that, for the purpose of convenient and brief description, for a detailed working process of the foregoing controller, network device, packet forwarding apparatus, and each module, refer to a corresponding process in the foregoing method embodiment. Details are not described herein.

[0471] It should be understood that the controller, the network device, and the packet forwarding apparatus provided in embodiments of this application may all be implemented by using an application-specific integrated circuit (application-specific integrated circuit, ASIC) or a programmable logic device (programmable logic device, PLD). The PLD may be a complex program logic device (complex programmable logic device, CPLD), a field-programmable gate array (field-programmable gate array, FPGA), generic array logic (generic array logic, GAL), or any combination thereof. Alternatively, the packet forwarding method provided in the foregoing method embodiment may be implemented by software. When the packet forwarding method provided in the foregoing method embodiment is implemented by software, modules in the foregoing controller and network device may also be software modules.

[0472] FIG. 24 is a schematic diagram of a structure of yet another packet forwarding apparatus according to an embodiment of this application. The packet forwarding apparatus may be used in a controller or a network device in the communication network shown in FIG. 1 or FIG. 7. For example, the packet forwarding apparatus may be used in the network device 02a, 02c, or 02d in FIG. 1 or FIG. 7, or may be used in the network device 02b shown in FIG. 1. As shown in FIG. 24, the packet forwarding apparatus may include: a processor 701, a memory 702, a network interface 703, and a bus 704. The bus 704 is configured to connect the processor 701, the memory 702, and the network interface 703. A communication connection to another device may be implemented through the network interface 703 (which may be wired or wireless). The memory 702 stores a computer program 7021, and the computer program 7021 is used to implement a plurality of application functions. When the modules shown in FIG. 13 to FIG. 23 are implemented by using software modules, programs corresponding to the software modules may be stored in the memory 702 of the network device.

[0473] It should be understood that in this embodiment of this application, the processor 701 may be a CPU, or the processor 701 may be another general-purpose processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA), a GPU, or another programmable logic device, a discrete gate or transistor logic device, a discrete hardware assembly, or the like. The general-purpose processor may be a microprocessor, any conventional processor, or the like.

[0474] The memory 702 may be a volatile memory or a nonvolatile memory, or may include both a volatile memory and a nonvolatile memory. The nonvolatile memory may be a read-only memory (read-only memory, ROM), a programmable read-only memory (programmable ROM, PROM), an erasable programmable read-only memory (erasable PROM, EPROM), an electrically erasable programmable read-only memory (electrically EPROM, EEPROM), or a flash memory. The volatile memory may be a random access memory (random access memory, RAM), used as an external cache. By way of example, and not limitation, RAMs in many forms may be used, for example, a static random access memory (static RAM, SRAM), a dynamic random access memory (DRAM), a synchronous dynamic random access memory (synchronous DRAM, SDRAM), a double data rate synchronous dynamic random access memory (double data rate SDRAM, DDR SDRAM), an enhanced synchronous dynamic random access memory (enhanced SDRAM, ESDRAM), a synchlink dynamic random access memory (synchlink DRAM, SLDRAM), and a direct rambus random access memory (direct rambus RAM, DR RAM).

[0475] The bus 704 may further include a power bus, a control bus, a status signal bus, and the like, in addition to a data bus. However, for clear description, various types of buses in the figure are denoted as the bus 704.

[0476] According to a first aspect, the processor 701 may be configured to: obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow, and send the correspondence to a first network device, where the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow. For a detailed processing process of the processor 701, refer to the foregoing method embodiment. For example, reference may be made to detailed descriptions of step 101 and step 102 in the embodiment shown in FIG. 2, or detailed descriptions of step 401 to step 404 in the embodiment shown in FIG. 6, or detailed descriptions of step 501 to step 505 in the embodiment shown in FIG. 10, or detailed descriptions of step 601 to step 604 and step 608 to step 611 in the embodiment shown in FIG. 11. Details are not described herein again.

[0477] According to a second aspect, the processor 701 may be configured to: receive a correspondence that is between a first application-aware identifier and a first network service and that is sent by the controller in the network, and if a received target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence, where the first application-aware identifier is generated by the controller based on a user requirement of the service flow. For a detailed processing process of the processor 701, refer to the foregoing method embodiment. For example, reference may be made to detailed descriptions of step 103 in the embodiment shown in FIG. 2, or detailed descriptions of step 405 to step 408 in the embodiment shown in FIG. 6, or detailed descriptions of step 506 to step 508 in the embodiment shown in FIG. 10, or detailed descriptions of step 606 and step 607 in the embodiment shown in FIG. 11. Details are not described herein again.

[0478] According to a third aspect, the processor 701 may be configured to: generate a first application-aware identifier of a target service flow based on a user requirement of the target service flow, and send the first application-aware identifier. The first application-aware identifier is used by a network device to encapsulate a target application-aware identifier of the target service flow in a service packet of the target service flow, and the target application-aware identifier is the first application-aware identifier, or a second application-aware identifier that is of the target service flow and that is generated by the network device. The first application-aware identifier corresponds to a first network service, the first application-aware identifier is used by the network device to forward the service packet of the target service flow by using the first network service, and the first network service meets the user requirement of the target service flow. For a detailed processing process of the processor 701, refer to the foregoing method embodiment. For example, reference may be made to detailed descriptions of step 201 and step 202 in the embodiment shown in FIG. 2, or steps performed by the controller or any network device in the embodiment shown in FIG. 6, FIG. 10, or FIG. 11. Details are not described herein again.

[0479] According to a fourth aspect, the processor 701 may be configured to: receive a first application-aware identifier sent by the controller, where the first application-aware identifier is generated based on a user requirement of a service flow, the first application-aware identifier corresponds to a first network service, and the first network service meets the user requirement of the service flow; and if the received target service flow is a service flow indicated by the first application-aware identifier, encapsulate a target application-aware identifier in a service packet of the target service flow, and forward the service packet in which the target application-aware identifier is encapsulated, where the target application-aware identifier is the first application-aware identifier or a second application-aware identifier matching the first application-aware identifier. For a detailed processing process of the processor 701, refer to the foregoing method embodiment. For example, reference may be made to detailed descriptions of step 405 to step 408 in the embodiment shown in FIG. 6, or detailed descriptions of step 506 to step 508 in the embodiment shown in FIG. 10, or reference may be further made to detailed descriptions of step 606 and step 607 in the embodiment shown in FIG. 11. Details are not described herein again.

[0480] According to a fifth aspect, the processor 701 may be configured to: perform, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result; and send the in-situ flow detection result and a target application-aware identifier of the target service flow to the controller in the network. The target application-aware identifier is generated based on a user requirement of the target service flow, and the in-situ flow detection result and the target application-aware identifier are used by the controller to analyze transmission performance of the target service flow. For example, reference may be made to detailed descriptions of step 301 and step 302 in the embodiment shown in FIG. 5, or detailed descriptions of step 405 to step 408 in the embodiment shown in FIG. 6, or detailed descriptions of step 506 to step 508 in the embodiment shown in FIG. 10, or detailed descriptions of step 606 and step 607 in the embodiment shown in FIG. 11. Details are not described herein again.

[0481] According to a sixth aspect, the processor 701 may be configured to: receive an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, where the in-situ flow detection result is obtained by the third network device by performing in-situ flow detection on a target service flow, and the target application-aware identifier is generated based on a user requirement of the target service flow; and analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier. For a detailed processing process of the processor 701, refer to the foregoing method embodiment. For example, reference may be made to detailed descriptions of step 303 in the embodiment shown in FIG. 5, or detailed descriptions of step 401 to step 404 in the embodiment shown in FIG. 6, or detailed descriptions of step 501 to step 505 in the embodiment shown in FIG. 10, or detailed descriptions of step 601 to step 604 and step 608 to step 611 in the embodiment shown in FIG. 11. Details are not described herein again.

[0482] FIG. 25 is a schematic diagram of a structure of yet another network device according to an embodiment of this application. The network device may be used in the communication network shown in FIG. 1 or FIG. 7. For example, the network device may be the network device 02a, 02c, or 02d in FIG. 1 or FIG. 7, or may be the network device 02b shown in FIG. 1. As shown in FIG. 25, the network device may include: a main control board 801 and at least one interface board (where the interface board is also referred to as a line card or a service board). For example, FIG. 25 shows an interface board 802 and an interface board 803. If there are a plurality of interface boards, a switching board 804 may be included, and the switching board 804 is configured to complete data exchange between the interface boards.

[0483] The main control board 801 is configured to implement functions such as system management, device maintenance, and protocol processing. The interface board 802 and the interface board 603 are configured to: provide various service interfaces (for example, a POS interface, a GE interface, and an ATM interface), and forward a packet. The main control board 801 mainly includes three types of functional units: a system management control unit, a system clock unit, and a system maintenance unit. The main control board 801, the interface board 802, and the interface board 803 implement interworking by using a connection between a system bus and a platform backboard. The interface board 802 includes one or more central processing units 8021. The central processing unit 8021 is configured to: control and manage the interface board 802, communicate with a central processing unit 8011 on the main control board 801, and forward a packet. A forwarding entry memory 8024 on the interface board 802 is configured to store a forwarding entry. The central processing unit 8021 may forward the packet by searching the forwarding entry stored in the forwarding entry memory 8024.

[0484] One or more physical interface cards 6023 included in the interface board 802 are configured to: receive a packet sent by a previous-hop node, and send a processed packet to a next-hop node based on an instruction of the central processing unit 8021. A specific implementation process is not described herein again. Specific functions of the central processing unit 8021 are not described herein again either.

[0485] It may be understood that a receiving module 021 and a sending module 022 in the network device may be located in the interface board 802, and an obtaining module 023, a determining module 024, a generation module 025, a detection module 026, and an encapsulation module 027 may be located in the main control board 801.

[0486] It may be further understood that, as shown in FIG. 25, in this embodiment, a plurality of interface boards are included, and a distributed forwarding mechanism is used. In this mechanism, a structure of the interface board 803 is basically the same as a structure of the interface board 802, and operations on the interface board 803 are basically similar to operations on the interface board 802. For brevity, details are not described again. In addition, it may be understood that in FIG. 25, the central processing unit 8021 and/or a network processor 8022 in the interface board 802 may be dedicated hardware or a chip, for example, an application-specific integrated circuit, to implement the foregoing functions. This implementation is usually referred to as a manner of using dedicated hardware or a chip for processing on a forwarding plane. In another implementation, the central processing unit 8021 and/or the network processor 8022 may alternatively use a general-purpose processor, for example, a general-purpose CPU, to implement the foregoing functions.

[0487] In addition, it should be understood that there may be one or more main control boards 801. When there are a plurality of main control boards, a primary main control board and a secondary main control board may be included. There may be one or more interface boards, and this device having a stronger data processing capability provides more interface boards. If there are the plurality of interface boards, the plurality of interface boards can communicate with each other by using one or more switching boards, and the plurality of interface boards can jointly implement load balancing and redundancy backup. In a centralized forwarding architecture, the device may not need the switching board, and the interface board provides a function of processing service data of an entire system. In a distributed forwarding architecture, the device includes the plurality of interface boards. Data exchange between the plurality of interface boards may be implemented by using the switching board, to provide a large-capacity data exchange and processing capability. Therefore, a data access and processing capability of the network device in the distributed architecture is better than that of the device in the centralized architecture. A specific architecture that is to be used depends on a specific networking deployment scenario. This is not limited herein.

[0488] In a specific embodiment, a memory 8012 and a memory 8024 may be a read-only memory (read-only memory, ROM), another type of static storage device that can store static information and instructions, a random access memory (random access memory, RAM), or another type of dynamic storage device that can store information and instructions, or may be an electrically erasable programmable read-only memory (electrically erasable programmable read-only memory, EEPROM), a compact disc read-only memory (compact disc read-only Memory, CD-ROM) or another compact disc storage, an optical disc storage (including a compact disc, a laser disc, an optical disc, a digital versatile disc, a Blu-ray disc, or the like), a magnetic disk or another magnetic storage device, or any other medium that can be configured to carry or store expected program code in a form of a instruction structure or a data structure and that can be accessed by a computer, but is not limited thereto. The memory 8024 in the interface board 802 may exist independently, and is connected to the central processing unit 8021 through a communication bus. Alternatively, the memory 8024 may be integrated with the central processing unit 8021. The memory 8012 in the main control board 801 may exist independently, and is connected to the central processing unit 8011 through the communication bus. Alternatively, the memory 8012 may be integrated with the central processing unit 8011.

[0489] The memory 8024 is configured to store program code, and the central processing unit 8021 controls and executes the program code. The memory 8012 is configured to store program code, and the central processing unit 8011 controls execution of the program code. The central processing unit 8021 and/or the central processing unit 8011 may implement, by executing the program code, the packet forwarding method that is applied to the network device and that is provided in the foregoing embodiment. The program code stored in the memory 8024 and/or the memory 8012 may include one or more software modules. The one or more software modules may be the functional modules provided in the embodiment shown in any one of FIG. 15 to FIG. 17 and FIG. 19 to FIG. 22.

[0490] In a specific embodiment, the physical interface card 6023 may be a type of apparatus that uses any transceiver, and is configured to communicate with another device or a communication network, for example, an Ethernet, a radio access network (radio access network, RAN), a wireless local area network (wireless local area network, WLAN), or the like.

[0491] An embodiment of this application further provides a computer-readable storage medium. The computer-readable storage medium stores instructions, and the instructions are executed by a processor to implement the method that is performed by a controller or a network device and that is provided in the foregoing method embodiment.

[0492] An embodiment of this application further provides a computer program product including instructions. When the computer program product runs on a computer, the computer is enabled to perform the method that is performed by a controller or a network device and that is provided in the foregoing method embodiment.

[0493] An embodiment of this application further provides a communication network. As shown in FIG. 1 and FIG. 7, the communication network includes: a controller 01 and at least one network device. For example, FIG. 1 shows a total of five network devices: a network device 02a to a network device 02e, and FIG. 7 shows a total of four network devices: a network device 02a and network devices 02c to 02e.

[0494] The controller 01 may implement steps performed by the controller in the foregoing method embodiments, and the network device may implement steps performed by any network device in the foregoing method embodiments.

[0495] Optionally, the controller 01 may be the controller shown in FIG. 13, FIG. 14, FIG. 23, or FIG. 24, or may include the packet forwarding apparatus shown in FIG. 17 or FIG. 18. The at least one network device may include the network device shown in any one of FIG. 15, FIG. 16, FIG. 20 to FIG. 22, and FIG. 24, or may include the packet forwarding apparatus shown in FIG. 17 or FIG. 19.

[0496] Optionally, the communication network may be an APN.

[0497] An embodiment of this application further provides a chip. The chip may be configured to implement the method performed by the controller or the network device provided in the foregoing method embodiments.

[0498] All or some of the foregoing embodiments may be implemented by software, hardware, firmware, or any combination thereof. When software is used to implement embodiments, the foregoing embodiments may be implemented completely or partially in a form of a computer program product. The computer program product includes one or more computer instructions. When the computer program instructions are loaded or executed on a computer, all or some of the processes or the functions according to embodiments of this application are generated. The computer may be a general-purpose computer, a dedicated computer, a computer network, or other programmable apparatuses. The computer instructions may be stored in a computer-readable storage medium or may be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions may be transmitted from a website, computer, server, or data center to another website, computer, server, or data center in a wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (DSL)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium may be any usable medium that can be accessed by the computer, or a data storage device, such as a server or a data center, integrating one or more usable media. The usable medium may be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, a DVD), or a semiconductor medium. The semiconductor medium may be a solid-state drive (solid-state drive, SSD).

[0499] The term "at least one" in this application means one or more, and the term "a plurality of' in this application means two or more than two. For example, a plurality of nodes means two or more than two nodes. The terms "system" and "network" are often used interchangeably in this specification. The term "and/or" mentioned in this specification represents that three relationships may exist. For example, A and/or B may represent the following three cases: Only A exists, both A and B exist, and only B exists. The character "/" usually indicates an "or" relationship between the associated objects.

[0500] The foregoing descriptions are merely optional implementations of this application, but the protection scope of this application is not limited thereto. Any equivalent modification or replacement readily figured out by a person skilled in the art within the technical scope disclosed in this application shall fall within the protection scope of this application. Therefore, the protection scope of this application shall be subject to the protection scope of the claims.

Claims

1. A packet forwarding method, applied to a controller in a network, wherein the method comprises:

obtaining, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow; and

sending the correspondence to a first network device, wherein the correspondence is used by the first network device to determine, based on the first application-aware identifier, the first network service used to forward a service packet of the target service flow.

2. The method according to claim 1, wherein the correspondence comprises an identifier of the first network service, and the identifier of the first network service comprises: a binding segment identifier and/or an identifier of a network slice.

3. The method according to claim 1 or 2, wherein the first application-aware identifier comprises at least one of a user identifier and an application identifier.

4. The method according to claim 3, wherein the first application-aware identifier further comprises at least one of a flow identifier, a service level agreement SLA level, or a service requirement.

5. The method according to any one of claims 1 to 4, wherein the method further comprises:
sending the first application-aware identifier of the target service flow to a second network device, wherein the first application-aware identifier is used by the second network device to encapsulate the application-aware identifier of the target service flow in the service packet of the target service flow if the second network device determines that a received service flow is the target service flow.

6. The method according to claim 5, wherein the method further comprises:
sending an identifier generation rule to the second network device, so that the second network device generates a second application-aware identifier of the target service flow according to the identifier generation rule, and the second application-aware identifier is used to match the first application-aware identifier to determine that the received service flow is the target service flow.

7. The method according to any one of claims 1 to 6, wherein the method further comprises:
obtaining the user requirement of the target service flow through a northbound interface.

8. The method according to any one of claims 1 to 7, wherein the method further comprises:

receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, wherein the target application-aware identifier is an application-aware identifier of a service flow to which the in-situ flow detection result belongs, and the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is generated by the network device; and

analyzing transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier.

9. The method according to claim 8, wherein the method further comprises:

displaying a performance indicator of the target service flow based on a target granularity, wherein the performance indicator indicates the transmission performance of the target service flow; and

the target granularity is a granularity indicated by at least one identifier in the target application-aware identifier.

10. The method according to claim 8 or 9, wherein the method further comprises:

determining, based on the transmission performance of the target service flow, that the first network service does not meet the user requirement of the target service flow;

determining that a network service required for transmitting the target service flow is a second network service; and

sending a correspondence between the first application-aware identifier and the second network service to the first network device.

11. The method according to any one of claims 8 to 10, wherein before the receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device, the method further comprises: sending a sending policy of the target service flow to the first network device and/or the third network device, wherein the sending policy indicates to report the in-situ flow detection result of the target service flow.

12. The method according to any one of claims 8 to 11, wherein the receiving an in-situ flow detection result and a target application-aware identifier that are sent by a third network device comprises: receiving the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier that are sent by the third network device; and

the analyzing transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier comprises:

determining, based on a correspondence between the target application-aware identifier and the in-situ flow detection flow identifier, at least one data flow comprised in the target service flow; and

analyzing, based on the in-situ flow detection result, transmission performance of the at least one data flow comprised in the target service flow.

13. The method according to any one of claims 1 to 12, wherein the user requirement of the target service flow comprises one or more of the following requirements: a requirement for a specified forwarding path, a requirement for a specified network slice, and a requirement for a performance indicator of transmission performance.

14. A packet forwarding method, applied to a network device, wherein the method comprises:

receiving a correspondence that is between a first application-aware identifier and a first network service and that is sent by a controller in a network, wherein the first application-aware identifier is generated by the controller based on a user requirement of a service flow; and

if the received target service flow is a service flow indicated by the first application-aware identifier, forwarding a service packet of the target service flow by using the first network service and based on the correspondence.

15. The method according to claim 14, wherein the method further comprises:

obtaining a second application-aware identifier of the target service flow from the service packet of the target service flow; and

if the second application-aware identifier matches the first application-aware identifier, determining that the target service flow is the service flow indicated by the first application-aware identifier.

16. The method according to claim 15, wherein the service packet received by the network device comprises in-situ flow information telemetry IFIT information, and the second application-aware identifier is encapsulated in a flow identifier field or a reserved field of the IFIT information; or

the second application-aware identifier is encapsulated in a destination address field, a hop-by-hop option header HBH, a destination option header DOH, or a segment routing header SRH of the service packet.

17. The method according to claim 16, wherein the second application-aware identifier is encapsulated in a binding segment identifier field of the SRH field.

18. The method according to claim 14, wherein the method further comprises:

receiving an identifier generation rule sent by the controller;

generating a second application-aware identifier of the target service flow according to the identifier generation rule; and

if the second application-aware identifier matches the first application-aware identifier, determining that the target service flow is the service flow indicated by the first application-aware identifier.

19. The method according to claim 18, wherein the service packet received by the network device comprises IFIT information; and the forwarding a service packet of the target service flow by using the first network service comprises:

encapsulating a target application-aware identifier in a flow identifier field or a reserved field of the IFIT information; and
forwarding, by using the first network service, the service packet in which the target application-aware identifier is encapsulated.

20. The method according to any one of claims 14 to 19, wherein if the service packet that is of the target service flow and that is received by the network device comprises in-situ flow detection information, the method further comprises:

performing in-situ flow detection on the target service flow based on the in-situ flow detection information, to obtain an in-situ flow detection result; and
sending the in-situ flow detection result and the target application-aware identifier to the controller, wherein the target application-aware identifier is the first application-aware identifier, or the second application-aware identifier that is of the target service flow and that is obtained by the network device.

21. The method according to claim 20, wherein the method further comprises: receiving a sending policy that is of the target service flow and that is sent by the controller, wherein the sending policy indicates to report the in-situ flow detection result of the target service flow; and
the sending the in-situ flow detection result and the target application-aware identifier to the controller comprises: sending the in-situ flow detection result and the target application-aware identifier to the controller based on the indication of the sending policy.

22. The method according to claim 20 or 21, wherein the sending the in-situ flow detection result and the target application-aware identifier to the controller comprises:
sending the in-situ flow detection result, the target application-aware identifier, and a corresponding in-situ flow detection flow identifier to the controller.

23. A controller, wherein the controller comprises a memory, a processor, and a computer program that is stored in the memory and that can be run on the processor, and when executing the computer program, the processor implements the method according to any one of claims 1 to 13.

24. A network device, wherein the network device comprises a memory, a processor, and a computer program that is stored in the memory and that can be run on the processor, and when executing the computer program, the processor implements the method according to any one of claims 14 to 22.

25. A computer-readable storage medium, wherein the computer-readable storage medium stores instructions, and the instructions are executed by a processor to implement the method according to any one of claims 1 to 22.

26. A communication network, wherein the communication network comprises a controller and a network device, the controller is configured to perform the method according to any one of claims 1 to 13, and the network device is configured to perform the method according to any one of claims 14 to 22.

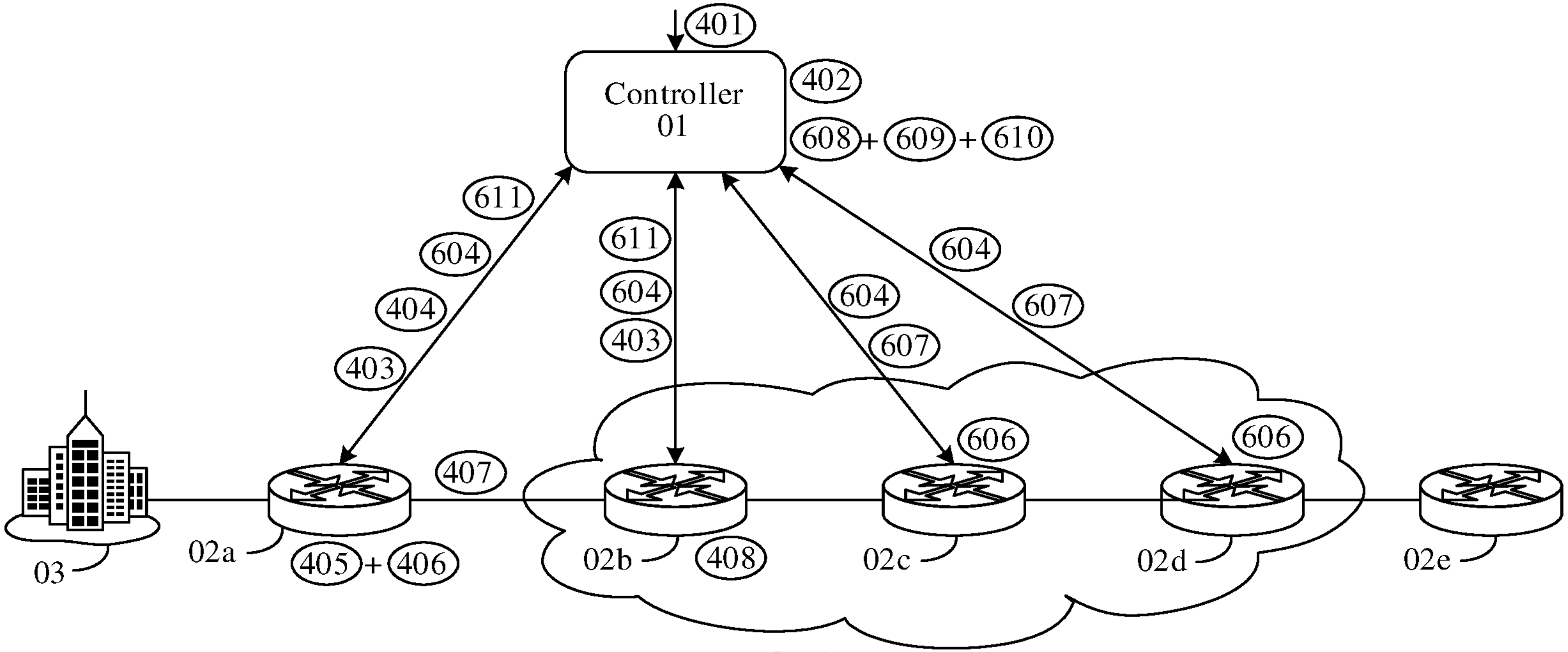

401
Controller
01
402
608
+
609
+
610
611
604
404
403
611
604
403
604
607
604
607
606
606
407
03
02a
405
+
406
02b
408
02c
02d
02e

FIG. 1

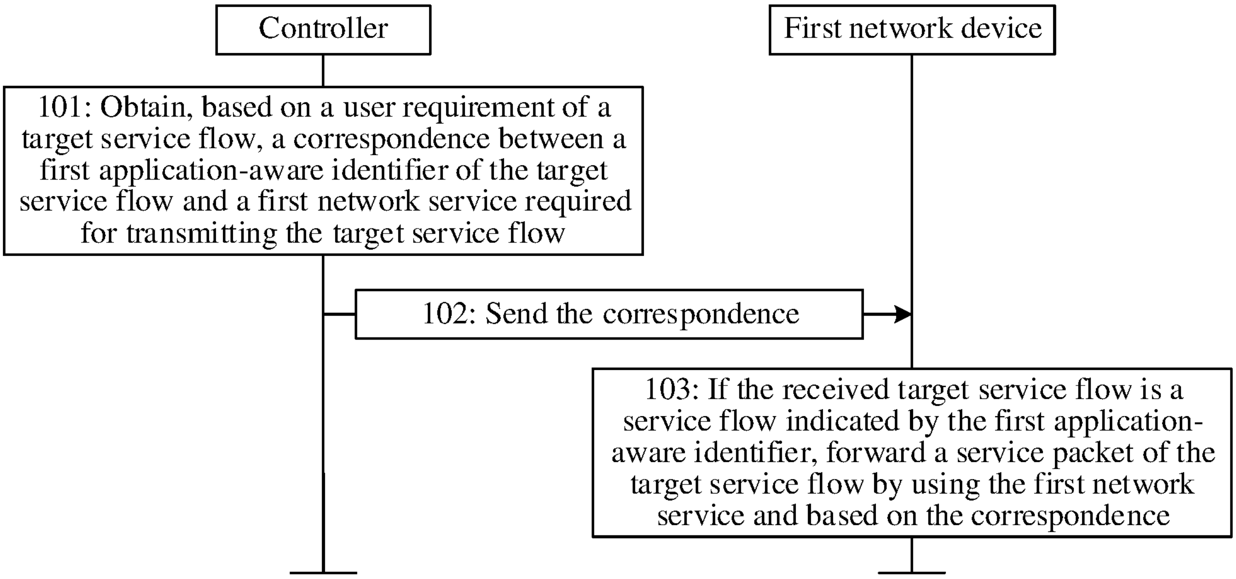
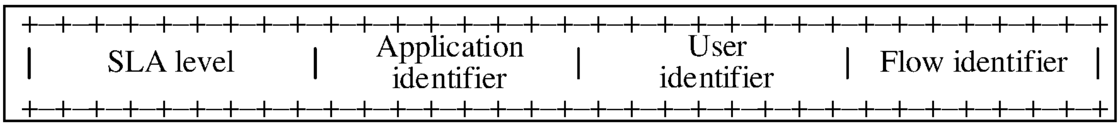

Controller
First network device
101: Obtain, based on a user requirement of a target service flow, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow
102: Send the correspondence
103: If the received target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence

FIG. 2



SLA level	Application identifier	User identifier	Flow identifier

FIG. 3

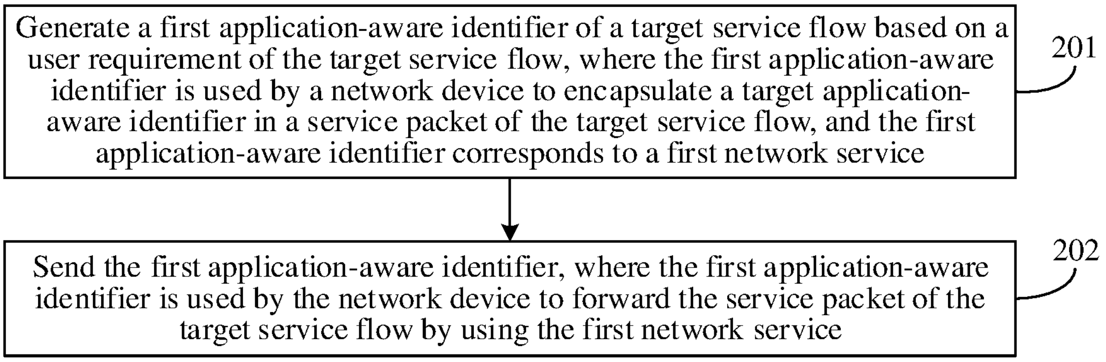

Generate a first application-aware identifier of a target service flow based on a user requirement of the target service flow, where the first application-aware identifier is used by a network device to encapsulate a target application-aware identifier in a service packet of the target service flow, and the first application-aware identifier corresponds to a first network service
201
Send the first application-aware identifier, where the first application-aware identifier is used by the network device to forward the service packet of the target service flow by using the first network service
202

FIG. 4

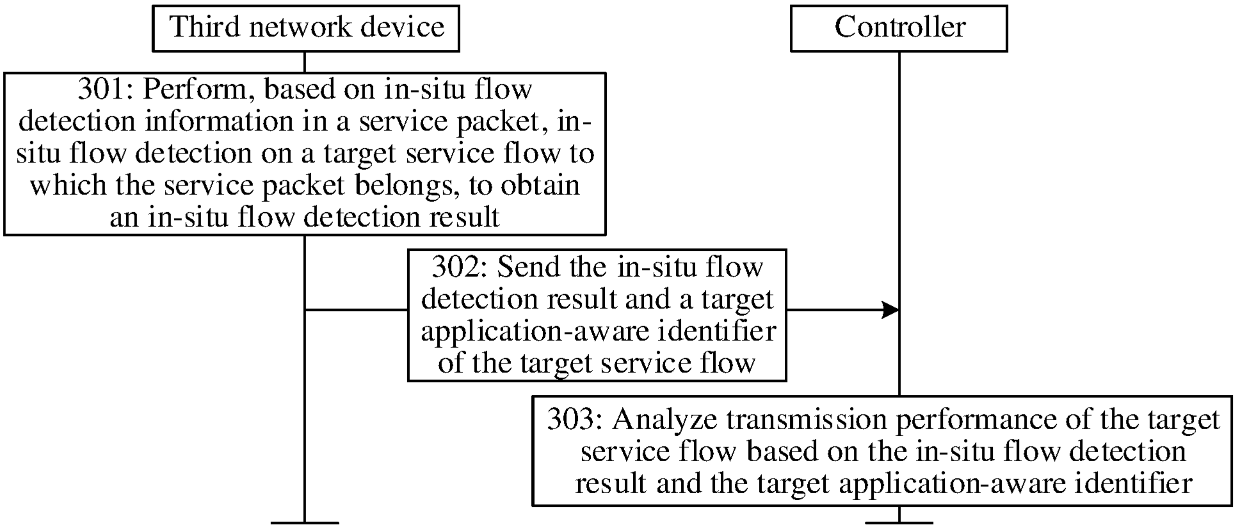

Third network device
Controller
301: Perform, based on in-situ flow detection information in a service packet, in-situ flow detection on a target service flow to which the service packet belongs, to obtain an in-situ flow detection result
302: Send the in-situ flow detection result and a target application-aware identifier of the target service flow
303: Analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier

FIG. 5

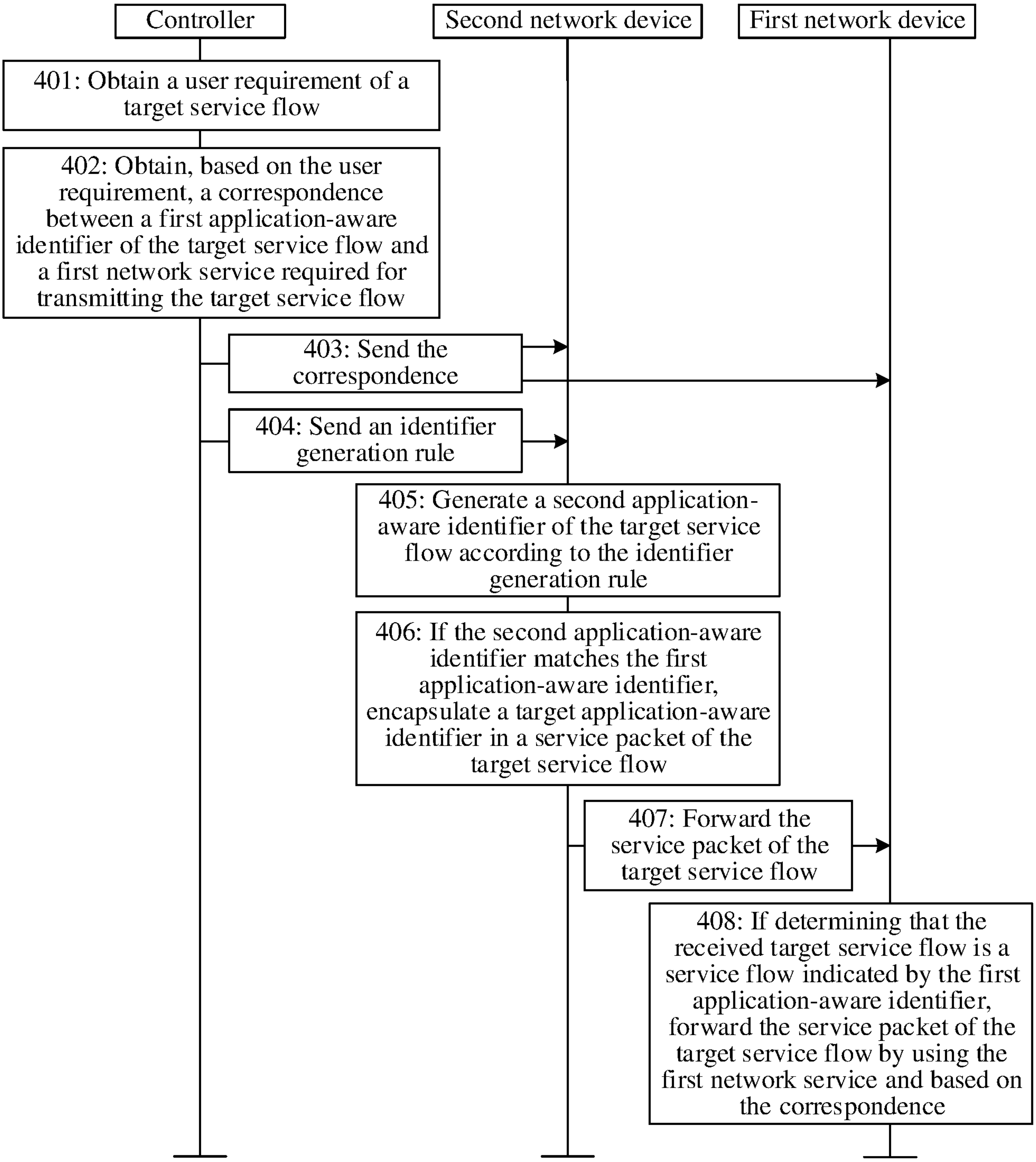

Controller
Second network device
First network device
401: Obtain a user requirement of a target service flow
402: Obtain, based on the user requirement, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow
403: Send the correspondence
404: Send an identifier generation rule
405: Generate a second application-aware identifier of the target service flow according to the identifier generation rule
406: If the second application-aware identifier matches the first application-aware identifier, encapsulate a target application-aware identifier in a service packet of the target service flow
407: Forward the service packet of the target service flow
408: If determining that the received target service flow is a service flow indicated by the first application-aware identifier, forward the service packet of the target service flow by using the first network service and based on the correspondence

FIG. 6

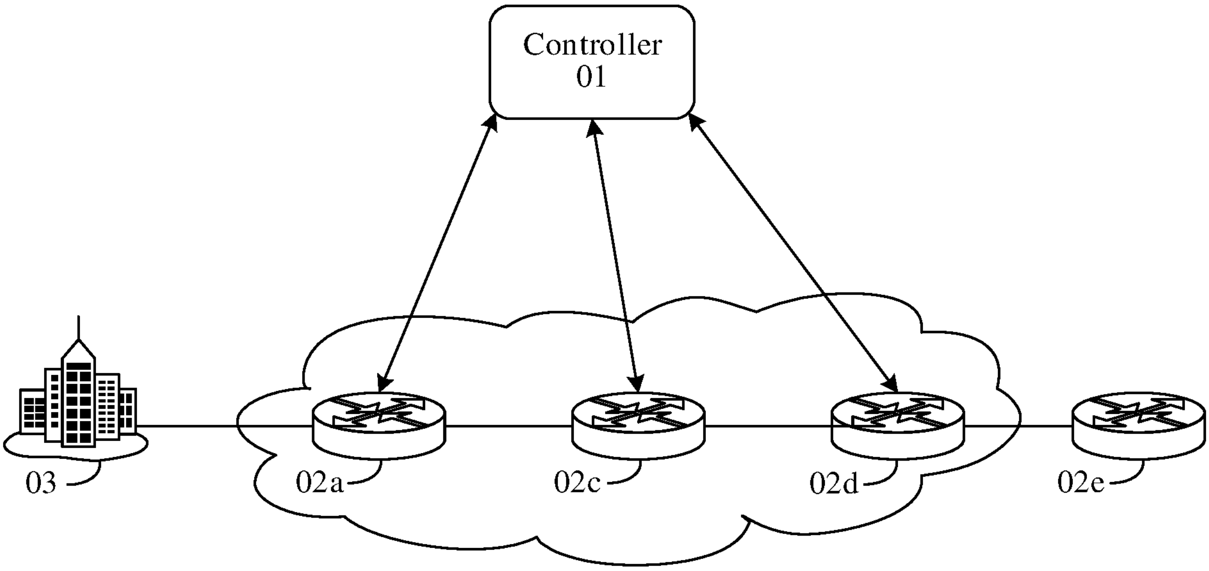


FIG. 7

SLA level	Application identifier	User identifier	Flow identifier	Arguments

FIG. 8

Locator address	Function identifier	Arguments

FIG. 9

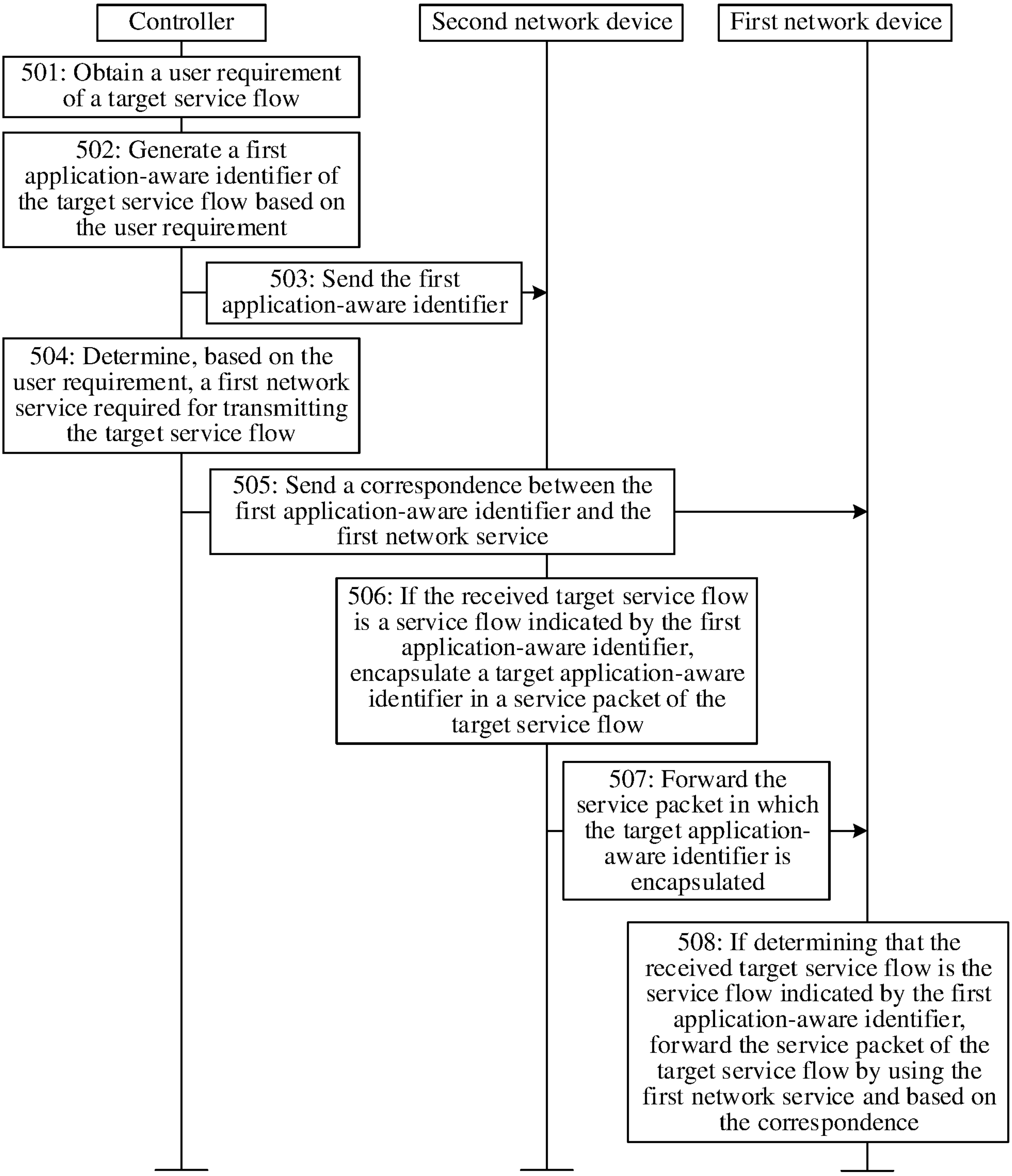

Controller
Second network device
First network device
501: Obtain a user requirement of a target service flow
502: Generate a first application-aware identifier of the target service flow based on the user requirement
503: Send the first application-aware identifier
504: Determine, based on the user requirement, a first network service required for transmitting the target service flow
505: Send a correspondence between the first application-aware identifier and the first network service
506: If the received target service flow is a service flow indicated by the first application-aware identifier, encapsulate a target application-aware identifier in a service packet of the target service flow
507: Forward the service packet in which the target application-aware identifier is encapsulated
508: If determining that the received target service flow is the service flow indicated by the first application-aware identifier, forward the service packet of the target service flow by using the first network service and based on the correspondence

FIG. 10

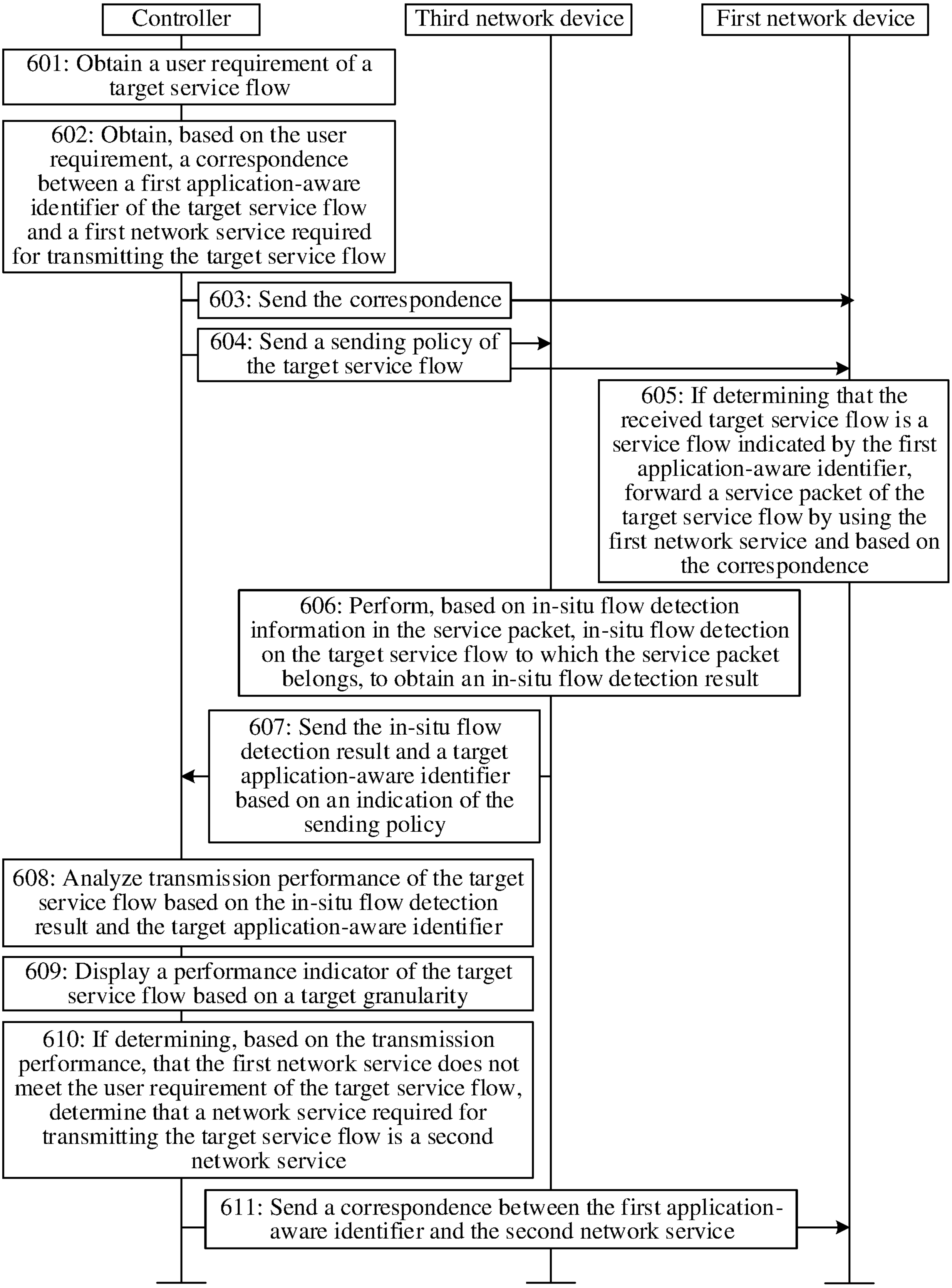

Controller
Third network device
First network device
601: Obtain a user requirement of a target service flow
602: Obtain, based on the user requirement, a correspondence between a first application-aware identifier of the target service flow and a first network service required for transmitting the target service flow
603: Send the correspondence
604: Send a sending policy of the target service flow
605: If determining that the received target service flow is a service flow indicated by the first application-aware identifier, forward a service packet of the target service flow by using the first network service and based on the correspondence
606: Perform, based on in-situ flow detection information in the service packet, in-situ flow detection on the target service flow to which the service packet belongs, to obtain an in-situ flow detection result
607: Send the in-situ flow detection result and a target application-aware identifier based on an indication of the sending policy
608: Analyze transmission performance of the target service flow based on the in-situ flow detection result and the target application-aware identifier
609: Display a performance indicator of the target service flow based on a target granularity
610: If determining, based on the transmission performance, that the first network service does not meet the user requirement of the target service flow, determine that a network service required for transmitting the target service flow is a second network service
611: Send a correspondence between the first application-aware identifier and the second network service

FIG. 11

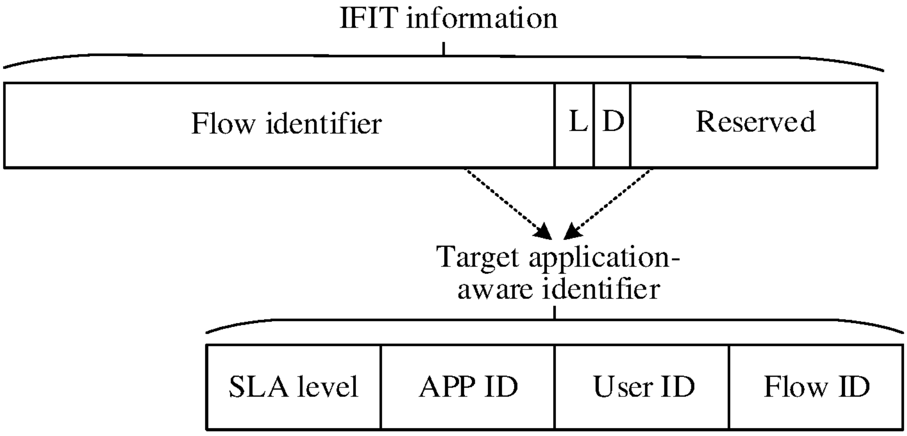


FIG. 12

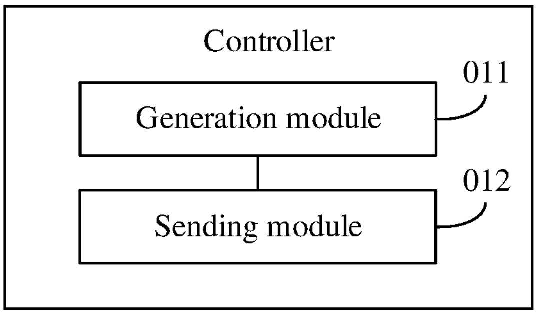


FIG. 13

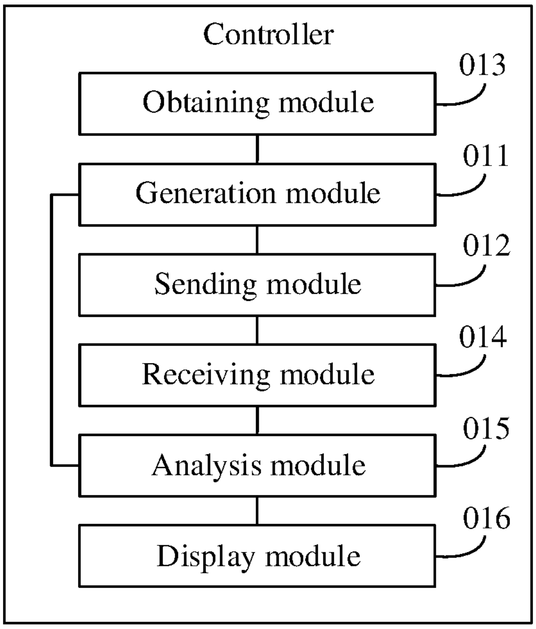


FIG. 14

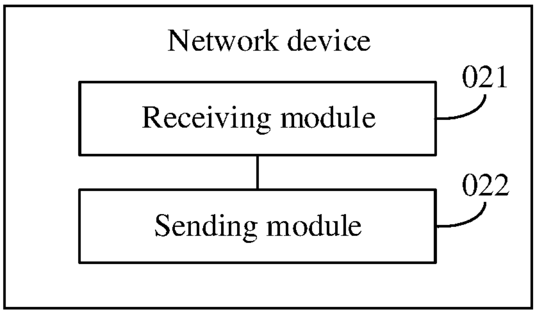


FIG. 15

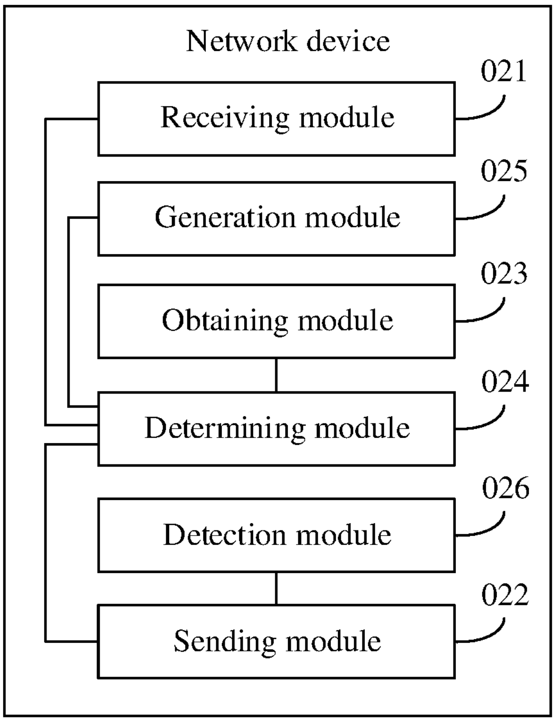


FIG. 16

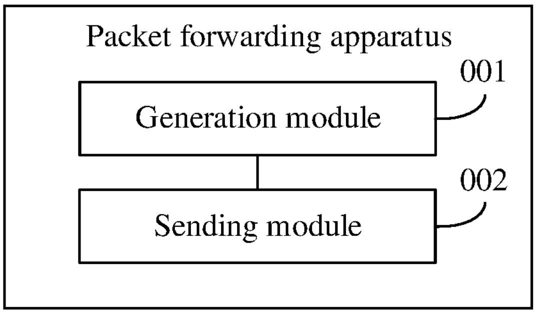


FIG. 17

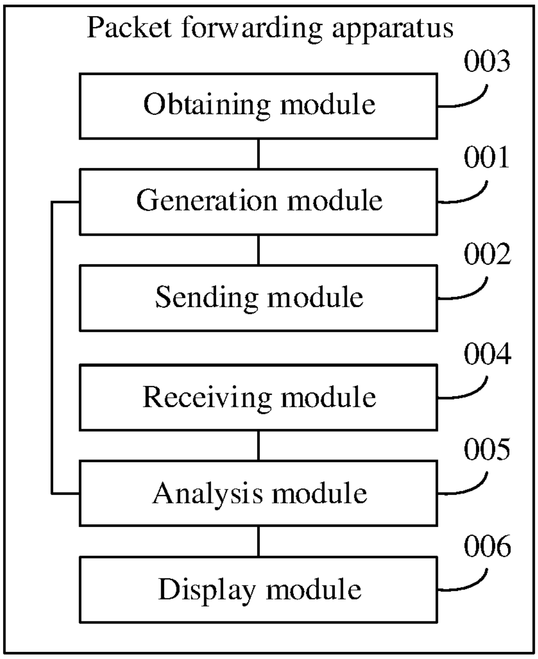

Packet forwarding apparatus
003
Obtaining module
001
Generation module
002
Sending module
004
Receiving module
005
Analysis module
006
Display module

FIG. 18

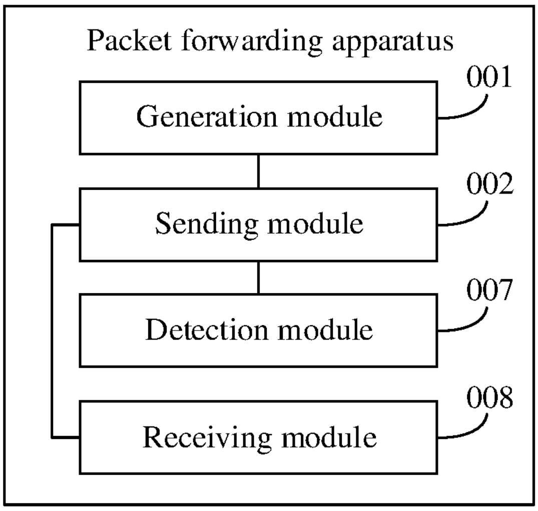

Packet forwarding apparatus
001
Generation module
002
Sending module
007
Detection module
008
Receiving module

FIG. 19

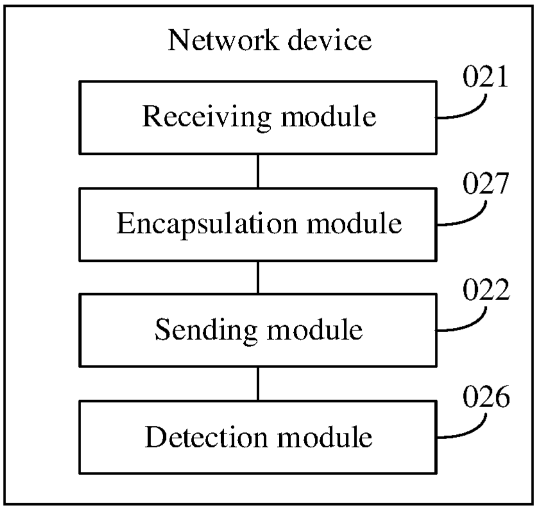


FIG. 20

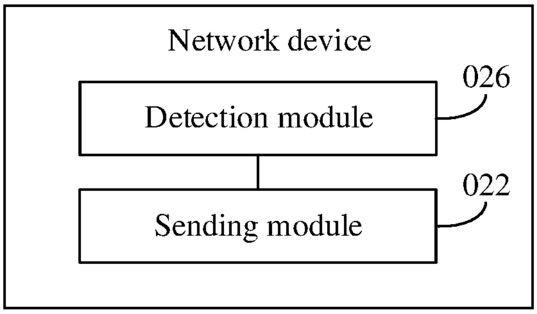


FIG. 21

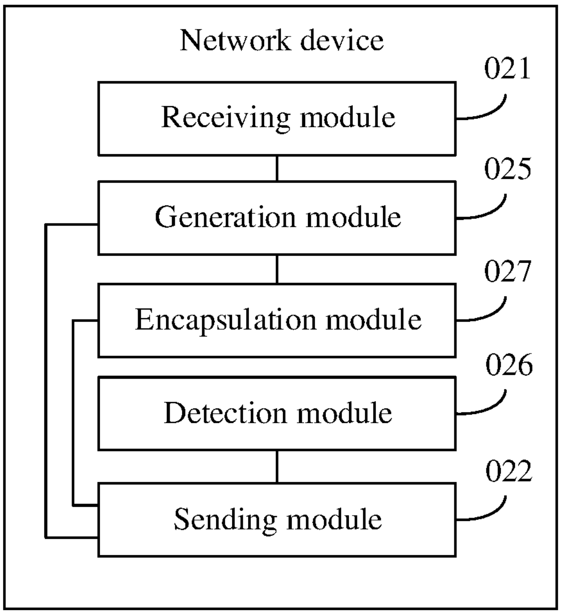


FIG. 22

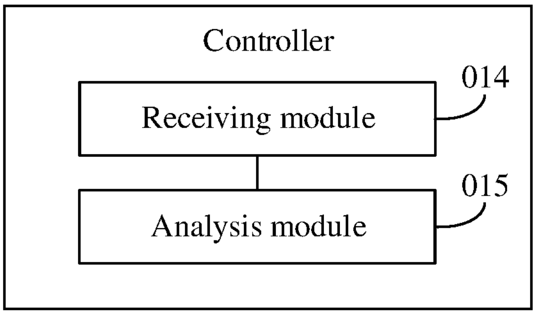

Controller
014
Receiving module
015
Analysis module

FIG. 23

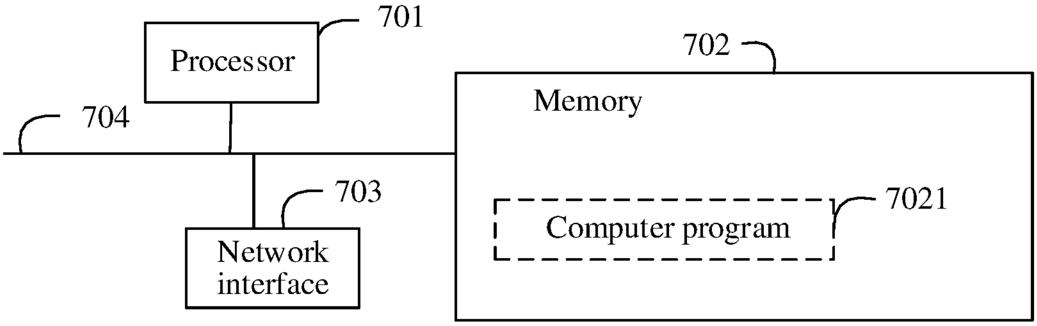

701
Processor
702
Memory
704
703
7021
Computer program
Network interface

FIG. 24

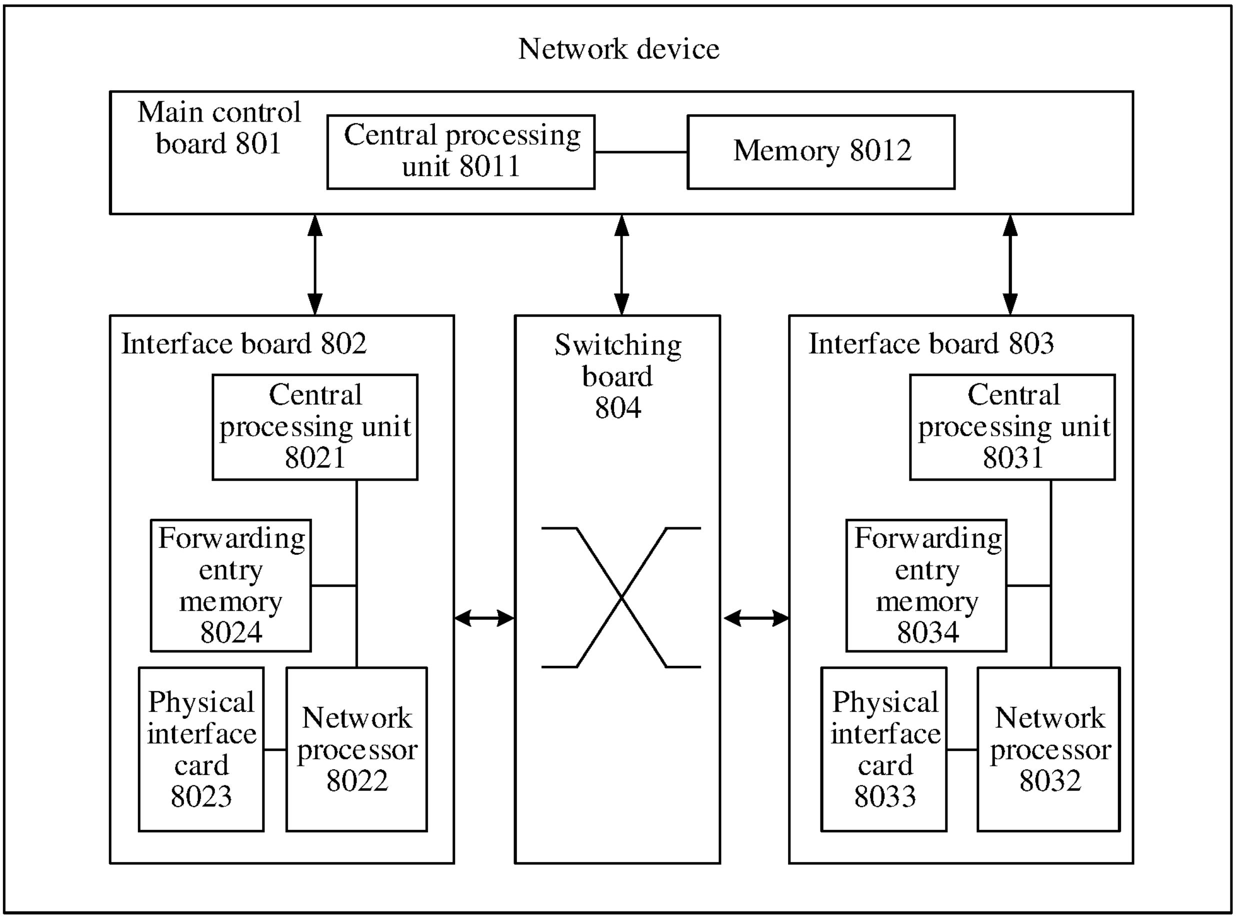

Network device
Main control board 801
Central processing unit 8011
Memory 8012
Interface board 802
Central processing unit 8021
Forwarding entry memory 8024
Physical interface card 8023
Network processor 8022
Switching board 804
Interface board 803
Central processing unit 8031
Forwarding entry memory 8034
Physical interface card 8033
Network processor 8032

FIG. 25

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/096052

A. CLASSIFICATION OF SUBJECT MATTER

H04W 76/10(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W76/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; ENTXTC; CNKI: 业务, 数据, 流, 转发, 发送, 对应, 关系, 映射, 匹配, 建立, 获取, 生成, 设置, 确定, 应用感知标识, 应用, 用户, 会话, 标识, ID, 网络服务, 绑定段, 网络切片, 转发路径, BSID, APN, 应用感知网络, application awareness networking, application-aware network, application aware network, 业务识别网络, DPI, deep packet inspection, 深度包检测, 深度分组检测 VEN; EPTXT; WOTXT; USTXT; IEEE; 3GPP: APN, application awareness networking, application-aware network, application aware network, DPI, deep packet inspection, forward+, transmit+, path, strategy, corresponding, map +, match+, service, business, flow, session, identification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 111654923 A (HUAWEI TECHNOLOGIES CO., LTD.) 11 September 2020 (2020-09-11) description, paragraphs [0128]-[0146]	1-26
Y	CN 111726839 A (HUAWEI TECHNOLOGIES CO., LTD.) 29 September 2020 (2020-09-29) description, paragraphs [0122]-[0129]	1-26
A	CN 101882999 A (ZTE CORP.) 10 November 2010 (2010-11-10) entire document	1-26
A	CN 105577638 A (INTEL CORP.) 11 May 2016 (2016-05-11) entire document	1-26
A	US 2016191348 A1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 30 June 2016 (2016-06-30) entire document	1-26

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search **13 July 2022**	Date of mailing of the international search report **16 August 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/096052

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2021084526 A1 (VIVO MOBILE COMMUNICATION CO., LTD.) 18 March 2021 (2021-03-18) entire document	1-26
A	WO 2018167359 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 20 September 2018 (2018-09-20) entire document	1-26

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/096052

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111654923 A	11 September 2020	WO 2017201722 A1	30 November 2017
		CN 109156040 A	04 January 2019
		IN 201837048409 A	18 January 2019
		BR 112018074138 A2	26 February 2019
		EP 3461071 A1	27 March 2019
		EP 3461071 A4	17 April 2019
		US 2019166634 A1	30 May 2019
		JP 2019521588 W	25 July 2019
		CN 109156040 B	28 April 2020
		JP 6727341 B2	22 July 2020
		EP 3461071 B1	09 December 2020
CN 111726839 A	29 September 2020	WO 2020187052 A1	24 September 2020
CN 101882999 A	10 November 2010	WO 2010127524 A1	11 November 2010
		CN 101882999 B	13 August 2014
CN 105577638 A	11 May 2016	US 2016127422 A1	05 May 2016
		DE 102015012569 A1	04 May 2016
		US 10015203 B2	03 July 2018
		CN 105577638 B	15 November 2019
US 2016191348 A1	30 June 2016	KR 20160042441 A	19 April 2016
		CN 105579990 A	11 May 2016
		JP 2016528630 A	15 September 2016
		WO 2015023256 A1	19 February 2015
		EP 3033687 A1	22 June 2016
		US 9954743 B2	24 April 2018
		EP 3033687 A4	05 July 2017
		EP 3033687 B1	03 July 2019
		JP 6162337 B2	12 July 2017
US 2021084526 A1	18 March 2021	CN 109041119 A	18 December 2018
		EP 3637844 A1	15 April 2020
		EP 3913967 A1	24 November 2021
		ES 2899395 T3	11 March 2022
		US 2022191732 A1	16 June 2022
		HU E056963 T2	28 April 2022
		PT 3637844 T	19 November 2021
		WO 2018223965 A1	13 December 2018
		US 11323912 B2	03 May 2022
		EP 3637844 A4	17 June 2020
		EP 3637844 B1	06 October 2021
		EP 3913967 A4	24 November 2021
WO 2018167359 A1	20 September 2018	None	

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 202110625901X **[0001]**